Journal of Innovation in Science and Engineering Research

(A Quarterly e-Journal)

Vol. 1 - No. 3 **December 2017** **ISSN: 2456-8619**

New Prince Shri Bhavani College of Engineering & Technology
Vengaivasal Main Road
Gowrivakkam, Chennai – 600073
Tamil Nadu, India
Phone: 044 22780404, 22780303
www.jiser.net
editor@jiser.net

PERFORMANCEOFMODEL FOOTINGIN GEOCELL REINFORCEDSAND BED AGAINST PULLOUT

S. Subathra*

*Assistant Professor, Department of Civil Engineering, New Prince Shri Bhavani College of Engineering and Technology, Chennai - 600073

ABSTRACT: The study reported in this paper deals with the performance of model circular footing in geocell reinforced bed with and without basal reinforcement against pullout load. A circular footing model with diameter, D = 100 mm was embedded at a height of 200 mm in medium dense sand bed (RD=54%) and tested by applying rate of pull of 0.01 mm/s. Geonet having tensile strength of 7.81 kN/m was used for making geocells. The width of the geocell was adopted as 2D and its thickness was varied as 0.25D, 0.5D and 0.75D. The increase in uplift capacity of model footing in geocell reinforced sand bed was 170% and the inclusion of additional planar layer of geonet (basal reinforcement) beneath the geocell enhanced the resistance further by of 30% i.e. the increase in the capacity was 200% over the capacity of footing in unreinforced sand bed. Hence the inclusion of geocell with and without basal reinforcement in sand enhanced the uplift capacity considerably. However the increase in pullout resistance was found to be marginal for the thickness of geocell more than 0.5D.

KEYWORDS: Geocell, Basal reinforcement, circular footing, uplift

INTRODUCTION

Generally foundations of tent type structures are subjected to uplift forces. The resistance of the footing against the uplift was offered by the self-weight of the footing and the soil above the footing within the rupture surface. Generally the uplift resistance of the footing was increased by increasing the geometrical features of the footing and depth of embedment. The above methods adopted for increasing the uplift resistance were quite uneconomical. Hence the research works were carried out for more feasible solution to increase the uplift resistance and as a result the inclusion of geosynthetics (Ravichandran et al., 2008; Sivaraman et al., 2014; Khatun and Chottopadhyay, 2010; and Choudhary and Dash, 2013) into the soil-footing system was found to be the better solution. In most of the research works, it was aimed at to enhance the uplift capacity of footings by geosynthetic reinforcement and was included as single or multiple layers; but the effects of geocell reinforcement on uplift capacity was not studied adequately. Therefore the present research work is carried out to study the performance geocell (three dimensional form of geosynthetics) system in increasing the uplift resistance of the footing. Also the effect of inclusion of basal reinforcement beneath the geocell layer was also analysed in this work. The objectives of the research work fulfilled by performing tests on circular model footing embedded in medium dense sand bed with geocell inclusion as reinforcement.

Details of test medium, geosynthetic material, experimental facility developed and procedure adopted for conducting tests are presented in the subsequent sections. Results of 1g model tests

conducted by varying the thickness of geocell with and without basal reinforcement are presented and discussed. Important conclusions drawn from the study are also included in this paper.

PROPERTIES OF MATERIAL

The test materials includes river sand and geosynthetics used for fabricating geocell. The properties of sand and geocell material are presented below:

Sand and Sand Bed

The test medium chosen for the study is a clean river sand. The minimum and the maximum unit weights were found to be 13.60 kN/m^3 and 17.98 kN/m^3 respectively. The specific gravity of the sand was found to be 2.65. It is classified as poorly graded sand (SP) based on Unified Classification System. Tests were conducted in medium dense sand, for which bed was prepared by compaction to achieve the relative density of 54%. The unit weight of the sand bed was 15.66 kN/m^3. The angle of internal friction of the medium sand was found to be 35°.

Geocell Material

The geocell used in this study was fabricated using locally available geonet material. The aperture opening of the geonet was diamond in shape and the opening size was 8 x 6 mm. The tensile strength of the material was found to be 7.7 kN/m at the strain of 20%. The extension was 3.2% for 50% of peak load value. Cylindrical shape geocell was fabricated manually using geonet material with diameter equal to twice the diameter of model foundation with thickness of 0.25D, 0.5D and 0.75D. The geocell thus made contains 24 pockets and the pockets were tied together using geosynthetic ties. Basal reinforcement used in the study was also made of same geonet material.

EXPERIMENTAL ARRANGEMENT

The Fig. 1 shows the experimental arrangement for the pullout tests. A model steel tank of size 740 mm x 740 mm x 650 mm was used to perform the tests. The steel tank was graduated for every 50 mm and was placed in a loading frame of capacity 50 kN. A separate loading yoke arrangement was made to pull the circular model footing of size 100 mm using a hydraulic jack of 100 kN capacity. The jack is operated manually using the hydraulic pump. A proving ring of 2.25 kN capacity was placed in between the loading yoke and the hydraulic jack to observe the mobilised pullout capacity. Dial gauges were placed on the plate connected to yoke to measure the displacement of footing. The travel length of the dial gauges was 50 mm with least count of 0.01 mm.

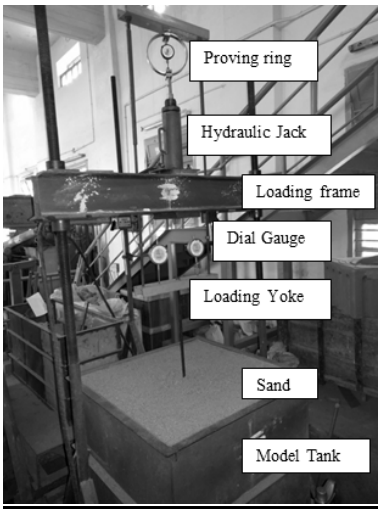

Fig. 1 Experimental arrangement for Pullout tests

The sand bed was prepared to the required density using sand pouring and compaction technique. The tests were conducted on footing embedded at a depth of 2D (=200 mm) from the sand bed surface. Once the desired depth was reached from the bottom of the tank, the footing arrangement which consists of the loading yoke was placed in position and sand was poured above the footing in layers and compacted to achieve required density of bed.

Test was conducted by uplifting the model footing by operating the jack at an approximate rate of 0.01 mm/s. The load and displacement readings were recorded at regular time interval continuously till the displacement of footing was 40mm.

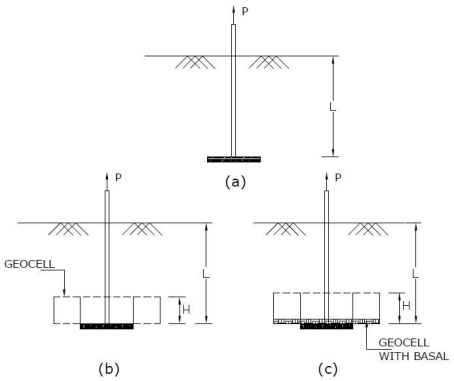

Fig. 2 Model Footing (a) Model Circular Footing, (b) Model Footing with Geocell Reinforcement and (c) Model Footing with Geocell+Basal Reinforcement.

In this research study three series of tests were conducted as shown in Fig. 2. First series of tests were on model footing without geocell inclusion. In the second and third series, tests were conducted in geocell inclusion but without basal and with basal reinforcement respectively.

In tests on reinforced cases the geocell was placed directly above the footing. In the case geocell with basal reinforcement, the basal reinforcement was placed beneath the geocell and tied together using the cable ties. The geocell with basal reinforcement was placed directly above the

footing (Fig. 2). The tests were carried out with both the configurations of reinforcement and compared with the results of unreinforced case to understand the effect of geocell reinforcement of both the configurations and the thickness of the geocell on pullout response.

RESULTS AND DISCUSSION

The pullout tests on the model footings embedded in the medium dense sand were conducted in unreinforced bed, geocell reinforced bed and geocell+basal reinforced sand bed. The results thus obtained are analysed in the following sequence: a) Load-displacement response of the footing in reinforced and unreinforced sand bed, b) Effect of the thickness of the geocell and c) Effect of inclusion of planar/basal reinforcement beneath the geocell.

1.1 Load-Displacement Response of Footing in Reinforced and Unreinforced Sand Bed

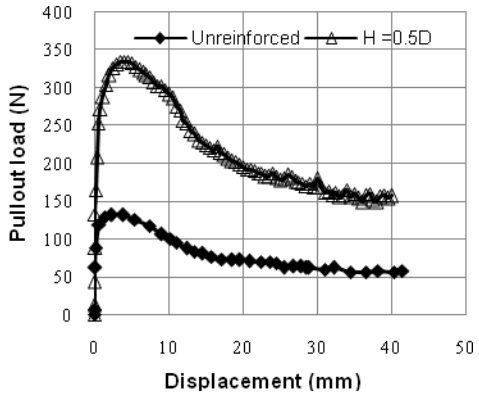

Fig. 3 Pullout response curves in medium dense sand bed

Fig. 3 shows the load response curves of the footing embedded in medium dense sand with and without reinforcement. In the unreinforced sand bed, the circular footing was embedded at 2D depth and the pullout tests were conducted. The load response curves shows three-phase behaviour with distinct pre-peak, post-peak and residual phases as reported by earlier researchers (Ravichandran et al., 2008; and Sivaraman et al., 2014) on anchors embedded in sand with inclusion of single and multi layers of geosynthetic reinforcements. In the pre-peak part of the curve, the pullout response (load) increases rapidly for a small increase in the displacement of footing. Once the peak had reached the resistance tend to decrease gradually. Further in the residual zone, the pullout resistance becomes almost constant value for the increase in displacement. In this case, the peak pullout load was found to be 131 N and the corresponding displacement was found to be 3.8 mm. The residual condition is reached at the displacement of 26mm with the pullout load of 57 N. The load-response curve of the reinforced case is similar in shape to that of the unreinforced case, but with increase in pullout and residual loads. The reinforced case with 0.5D of geocell thickness had contributed in improving the pullout and residual loads to 334 N and 156 N respectively. But the rate of reduction in the pullout load is higher in the post-peak phase of the curve when compared with the unreinforced case. The percentage of improvement was found to be nearly 173%.

1.2 Effect of Thickness of the Geocell

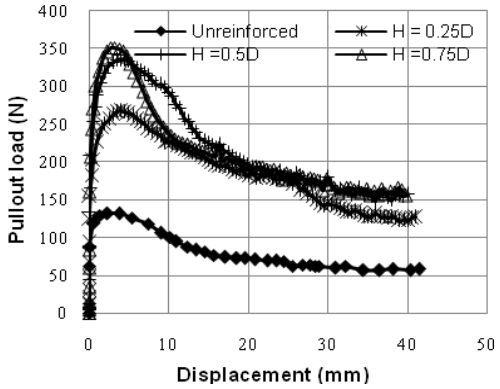

Fig. 4 Pullout response curves in medium dense sand bed for varying thickness

Fig. 4 shows the pullout load response curves of the circular anchor tested for the cases of reinforced and unreinforced conditions in medium dense sand bed. In the case of reinforced condition the thickness of the geocell adopted was 0.25D, 0.5D and 0.75D. The peak pullout load (P_u) corresponds to the displacement (□), residual pullout load (R) and the improvement are compared with the unreinforced state (URF) in Table 1. From Table 1 it could be seen that by increasing the thickness from 0.25D to 0.5D there was a significant increase in the peak pullout load. When the thickness of the geocell was further increased (i.e., 0.5D to 0.75D), the increase was insignificant. From the above results, it is understood that the increase in the peak pullout capacity is marginal for the geocell thickness more than 0.5D.

Table 1 Comparison of Peak load and displacement for various thickness of geocell reinforcement with unreinforced condition.

H	P_u (N)	δ (mm)	Improvement (%)	R (N)
URF	131	3.8	-	57
0.25D	267	4	121	126
0.5D	334	3.5	173	156
0.75D	350	2.8	171	155

1.3 Effect of Inclusion of Planar/Basal Reinforcement Beneath the Geocell Layer

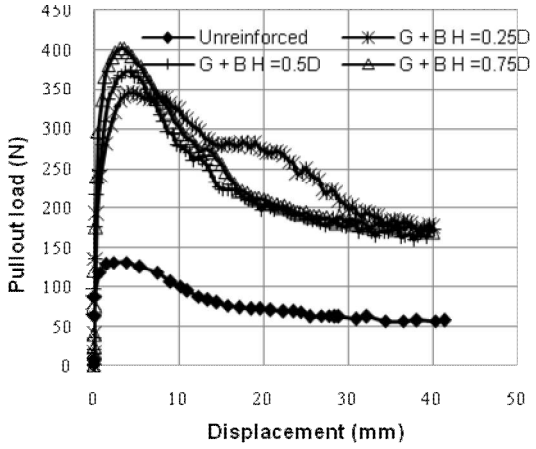

Fig 5 Pullout response curves in medium dense sand with geocell+basal reinforcement of varying thickness

The pullout response curves of footing in the medium dense sand bed reinforced with geocell+basal arrangement (G+B configuration) for different thickness of geocell shown in Fig. 5. The load-displacement curves are almost similar to that of the unreinforced and geocell reinforced cases. But due to the inclusion of basal reinforcement at the base of the geocell, the peak pullout load increases by 30%. In the geocell reinforcement, the bottom portion of the reinforcement is left open, hence the sand from the pockets of outer ring flows easily through the bottom.In case of G+B configuration, the basal reinforcement inclusion reduces the free flow of sand through the bottom opening of geocell pockets while pulling the footing, apart from adding stiffness to the geocell-sand reinforcement system, thus increased the pullout capacity.

Pullout resistance of footing for the two types of reinforcement configurations adopted in the present research are compared in Fig. 6 for the thickness of 0.25D, 0.5D and 0.75D. The pullout capacity is increased by the inclusion of basal layer of reinforcement to the geocell. In addition increase in pullout capacity with thickness of geocell is not significant for the geocell with thickness more than 0.5D for the density of sand considered in this study.

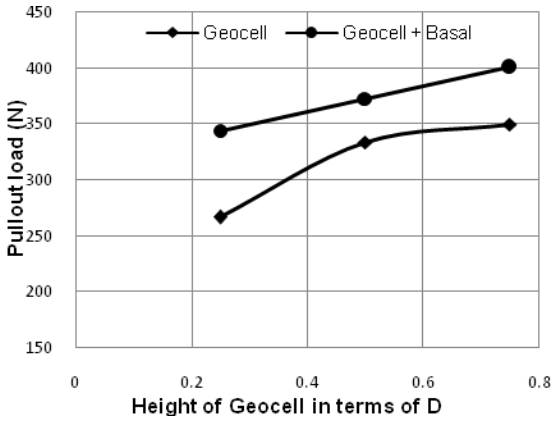

Fig. 6 Comparison of peak pullout loads between the two reinforcement configurations adopted.

CONCLUSION

The provision of geocell improves the pullout capacity of the model footing due to the stiffness of the geocell-soil system. The volume of the rupture surface is increased which increase the weight of the soil mass above the anchor, thus ensuring the improvement in the pullout load capacity. The effect of thickness is less pronounced beyond 0.5D. Addition of the planar layer beneath the geocell contributes reasonably well to the pullout capacity by increasing the stiffness of the system.

References

Choudhary A.K., and Dash S.K. (2013), 'Uplift behaviour of horizontal plate anchors embedded in geocell reinforced sand', Proceedings of Indian Geotechnical Conference, Roorkee, 1-5, 2013.

Khatun S. and Chottopadhyay B.C. (2010), 'Uplift capacity of plate anchor with reinforcement', Indian Geotechnical. Conference., Dec. 821-825, 2010.

Ravichandran P.T., Ilamparuthi K., and Toufeeq, M.M. (2008), 'Investigation on uplift behaviour of plate anchor in reinforced sand bed', Electronical Journal of Geotechnical Engineering, Vol. 13, pp. 1-8.

Sivaraman S., Ilamparuthi K. and Kishorkumar V. (2014), 'Uplift response of single and multiple anchors in reinforced sand bed', Proceedings of Indian Geotechnical Conference, December 18-20, Kakinada, India.

RESPONSEOFSINGLE PILEDUE TO DEEP EXCAVATION AND UNDERGROUND OPENINGS

A. Magesh*

*Assistant Professor, Department of Civil Engineering, New Prince Shri Bhavani College of Engineering and Technology, Chennai - 600073

ABSTRACT: One of the important issues of excavation and tunneling in urban areas is the assessment of its impact on foundations of neighbouring structures due to ground movements in particular on pile foundations. Excavation and tunneling operations cause lateral soil movements which induce additional lateral loads on piles and they are known as passive piles. They are subjected to additional bending moment and shear force which can lead to serviceability problems or even failure of piles itself. The present study focuses on 1g model tests to determine the response of single pile adjacent to a tunnel and a combined effect of excavation and tunneling. The effect of various parameters related to the pile, tunnel and soil on the response of pile to passive loading was analyzed in this study. The following parameters viz. pile length to diameter ratio, distance between pile and retaining wall, distance between pile and tunnel springline, position of pile with respect to retaining wall and tunnel are varied to understand the response of piles and also to identify the factor which influences the response most. The lateral deflection of pile head was measured. Analysis of the test results showed that the shorter pile (L/d =10) deflects more when compared to a long pile (L/d =20) in case of excavation, tunneling and combined case.

KEYWORDS: Pile, Tunnel, excavation, lateral soil movement.

INTRODUCTION

Excavation below ground level causes relaxation of in-situ stress due to ground movement. Tunneling is one form of excavation which causes ground movement. These ground movements affect the performance of structures located nearby such underground activity particularly the foundations of structures. The various field conditions in which piles are subjected to lateral soil movements are piles located adjacent to deep excavations, and tunnel construction, embankment construction and piles adjacent to pile installation operations. The lateral forces induced on piles due to soil movements as a result of situations stated above are termed as “passive loads” and the piles are termed as passive piles.

The lateral forces acting on piles due to soil movement may induce additional stresses and excessive deflection on the piles. In critical situations, they might damage the pile and compromise the stability and serviceability of supported structures. Thus, it is essential to evaluate pile responses due to lateral soil movements. Reasonably good number of research works are reported in literature for the prediction of ground movement due to excavation as well as tunneling and response of pile foundations towards these ground movements independently.

Both 1g model tests (Chen et al., 1995; Ilamparuthi and Madhumathi, 2011; Meguid and Mattar, 2009, etc.,) and centrifuge model tests (Leung et al., 2000) have been performed. Analysis were also carried out on numerically simulated models by researchers (Poulos and Chen, 1997; Chen et al., 2000; Min et al., 2011; Basile, 2014; etc.,) to understand the response of piles due to excavation and tunneling. However, the response of piles due to combined effect of excavation and tunneling has not been investigated adequately. Thus the combined effect of ground movement due to excavation and tunneling on pile is investigated in this research study through 1g model tests. The objective of the present study is to investigate the response of single pile to lateral soil movement by varying the pile length to diameter ratio, distance between pile and retaining wall, distance between the pile and tunnel springline, depth of tunnel and location of pile with respect to retaining wall and tunnel.

EXPERIMENTAL FACILITY

The experimental facility includes model tank, laboratory models of pile, retaining wall and tunnel and necessary instrumentation.

Experimental Procedure

The response of single pile due to tunneling is studied using a model tank of dimension 0.7 m x 0.29 m x 0.44 m made of steel. Aluminum hollow tubes of 19 mm outer diameter with 1 mm wall thickness were used to fabricate the piles with length to diameter ratio of 10 and 20. Retaining wall is made out of aluminum sheet 1.2 mm thick. Poorly graded sand with specific gravity 2.65 was used for experiments under medium dense condition with density 16.5 kN/m^3. Tunnelling operation is performed along the shorter side of the tank. The tunnel axis depth is normalized by taking the ratio of depth of tunnel axis to diameter of tunnel. Two normalized depths having H/D ratio 2.2 and 4.2 are considered in the experiments where H is the depth of tunnel axis from surface of sand bed and D is the tunnel diameter. Schematic arrangement of test setup is as shown in Fig. 1.

The tunnelling operation is simulated using a helical auger which is rotated at a uniform rate to cut through the soil. A hollow tube made of tin with outer diameter 74 mm and thickness of 0.5 mm is used as the liner. The auger was manually rotated at a uniform rate with a handle along with the liner. As the auger cuts the sand and moves forward, thrust was applied to the walls of the liner while operating the auger. Thus the liner moves along with the auger as in tunnel boring machine. The liner prevents the flow of sand during tunnel boring and the helical auger brings out the cuttings through the space between liner and auger. The experimental investigation on response of single pile due to excavation and tunnelling is observed by simulating an excavation operation first followed by tunnelling. The location of pile is changed in such a way that in first case, pile is located equidistant from retaining wall and tunnel springline.

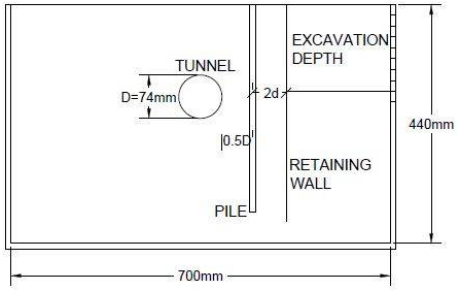

Fig. 1 Schematic Arrangement of Test Setup for Excavation and Tunneling

In the second case pile was located at a distance of 10d from the retaining wall. Sand in front of the retaining wall was removed manually in layers of 20 mm each. This will induce movements in retaining wall and pile due to the lateral pressure exerted by the soil behind it. The excavation is continued upto a depth of 200 mm. Deflections were noted for every 20 mm depth of excavation. Once the excavation activity was completed, the tunnel was bored to a length of 250 mm by adopting procedure as explained in previous para. Pile deflections for various length of penetration of tunnel was observed.

RESULTS AND DISCUSSION

In all the tests pile was located at a distance of 145 mm from the edge of the tank (mid-width of the tank). The deflection of the pile head are observed for two different tunnel axis depths and six different pile tip locations as shown in Fig. 2.

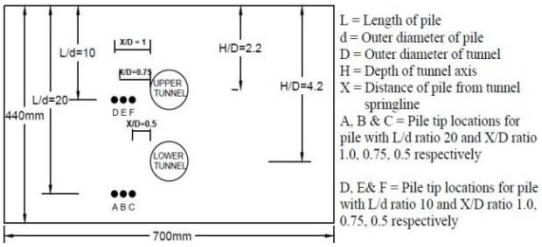

Fig. 2 Location of Pile tip and Tunnel axis

The variation of pile head deflection with respect to depth of penetration of tunnel for H/D = 2.2 is shown in Fig. 3. The maximum pile head deflection decreases when the distance of pile from tunnel springline increases for the condition of the sand bed and L/d ratio of pile.

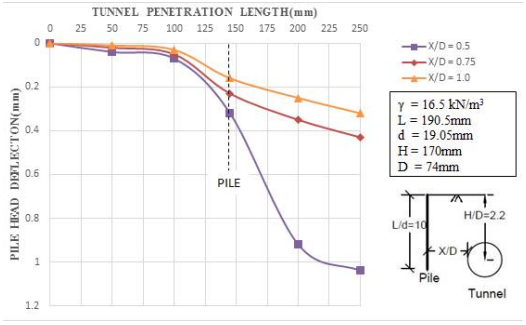

Fig. 3 Pile Head Deflection Vs Penetration Depth for L/d = 10, H/D = 2.2

The rate of pile head deflections shows steady increase after 100 mm of tunnel penetration irrespective of the distance of pile from the springline. This confirms the fact that, as the tunnel face approaches the pile, rapid soil movement occurs in the vicinity of the pile causing increase in pile head deflection. Fig. 4 shows variation of pile head deflection vs penetration depth for H/D = 4.2. The maximum value of pile head deflection is lesser compared to the previous case (H/D=2.2). As the tunneling operation is performed at a deeper depth (i.e. H/D = 4.2) the soil around the entire length of pile is subjected to movement which resulted in overall vertical movement of pile. Hence the lateral deflection of pile head has reduced for shorter pile when tunneling is performed at deeper depth. The location of pile is indicated with a dashed line. A comparison of Fig. 3 and Fig. 4 also confirms that the rate of pile head deflection is higher within a distance of 0.75 times diameter of tunnel from the center of the pile.

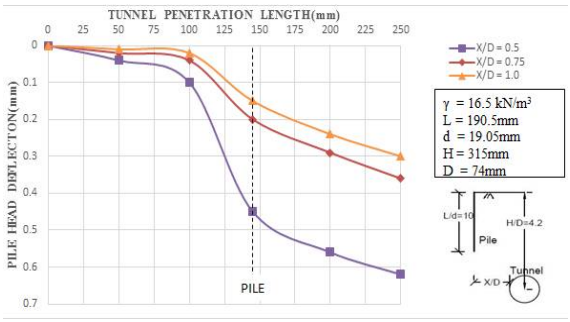

Fig. 4 Pile Head Deflection Vs Penetration Depth for L/d = 10, H/D = 4.2

Fig. 5 shows the comparison of maximum pile head deflection for pile with L/d ratio 20 located at a distance of X/D = 0.5 from tunnel springline under two depths (H/D=2.2, 4.2) of tunneling. The dashed line in indicates the position of pile which is at 145 mm from the edge of the tank. Maximum deflection in the pile for tunnel at H/D=2.2 was 4.5 times lesser when compared to the tunnel axis at H/D =4.2. When the length of pile extending below the tunnel axis is more, pile head deflection decreases because a significant part of the pile is embedded in sand which does not undergo movement due to tunneling. The rate of pile head deflection is very high between 100 mm to 200 mm penetration. This implies that within a distance of 0.75 times diameter of the tunnel from the center of pile, the rate of increase in pile head deflections are maximum.

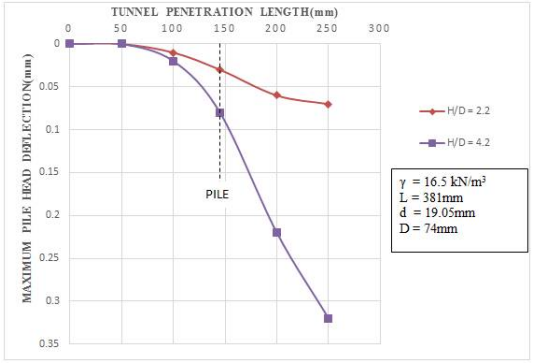

Fig. 5 Maximum pile head deflections for Tunnels with H/D=2.2 & 4.2

The variation of pile head deflection for combined condition of excavation and tunneling is studied at four different tip locations of the pile as shown in Fig. 6, where A,B,C and D are the tip locations of the pile. Tunneling was performed at H/D ratio 2.2.

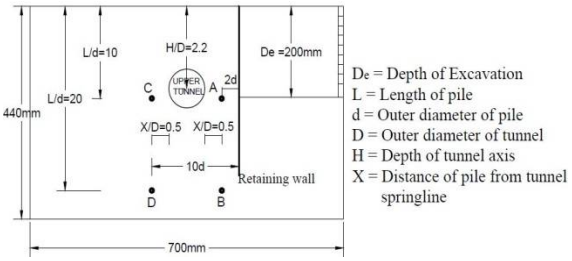

Fig. 6 Location of Pile tips for Excavation and Tunneling Case

Pile head deflection for every 20 mm excavation is recorded and continued up to 200 mm of excavation. Once excavation operation was completed tunneling process was commenced. The deflections of the pile for case A, B, C and D are shown in Table 1. For pile tip at A the pile head deflection was 5.3 mm for the pile at 2d distance from the excavation face and for the excavation depth of 200 mm. Thereafter the pile head deflection remained constant till a tunnel penetration length of 100 mm was achieved. Beyond 100 mm of penetration the pile deflected slightly towards the tunnel. As the face of the tunnel approached the pile, the soil movements around the pile increased causing deflection of pile head towards the tunnel side. Thus, deflection reduced to 5.23 mm when the maximum penetration distance of 250 mm is reached. During boring the tunneling the pile head deflection remains the same without any change in deflection till the distance between the tunnel face and pile is 0.6D approximately.

Table 1 Pile Head Deflection due to Excavation followed by Tunneling for Pile Tip at A, B, C and D

Depth of Excavation (mm)	Tunnel Penetration Distance (mm)	Pile Head Deflection(mm)			
		Pile Tip at A	Pile Tip at B	Pile Tip at C	Pile Tip at D
40	0	0	0	0	0
80	0	0.03	0.02	0	0
160	0	2.80	0.25	0	0
200	0	5.30	0.60	0	0
200	100	5.30	0.60	0.01	0.05
200	200	5.23	0.60	0.06	0.90
200	250	5.23	0.60	0.07	1.0

Unlike the case of short pile, long pile did not undergo deflection due to tunneling. It is observed that the stress condition in the part of pile extending below the tunnel is not affected significantly. Thus embedment of pile in this region provided sufficient resistance against deflection. When the pile tip is located at C and D zero deflection is recorded which shows that there is no influence of excavation when pile is located at 10 times the diameter of pile from the face of the excavation.

CONCLUSION

- The maximum lateral pile head deflection decreases when the distance of pile from tunnel springline increases for the condition of the sand bed and L/d ratio of pile.
- Lateral deflection of pile head is observed to be higher for short pile with less embedment depth when compared to a long pile.
- The magnitude of pile head deflection increased when the normalized depth of tunneling is increased from 2.2 to 4.2 for long pile (L/d=20). Whereas, for a short pile with L/d = 10 the magnitude of lateral deflection of pile decreased with increase in normalized depth of tunneling due to vertical settlement of pile.
- The rate of increase in pile head deflections are maximum when the advancing tunnel face is at a distance of 0.75 times diameter of the tunnel from the center of the pile.
- The net deflection of short pile when excavation and tunneling are performed on either side of the pile at equal distance is observed to be lesser than the total deflection when excavation alone is performed.
- In case of long pile with L/d = 20, the deflection due to tunneling is observed to be zero. Hence the net deflection is same as the deflection due to excavation alone.
- Zero pile head deflection due to excavation was observed for a pile at 10d from the retaining wall and 0.5D from the tunnel springline.

REFERENCES

- Basile F. (2014), 'Effects of tunneling on pile foundations', Soils and Foundations, Vol. 54, No.3, pp. 280–295.
- Chen L.T., Poulos H.G. and Hull T.S. (1995), 'Model tests on single piles subjected to lateral soil movement', Soils and Foundations, Vol. 37, No.1, pp. 1–12.
- Chen L.T., Poulos H.G. and Loganathan N. (2000), 'Pile responses caused by tunneling', Journal of Geotechnical and Geoenvironmental Engineering, ASCE, Vol. 125, No.3, pp. 207-215.
- Ilamparuthi K. and Madhumathi R.K. (2011), 'Effect of ground movement on the performance of pile foundation', Proceedings of Indian Geotechnical Conference, Kochi, Vol. 1, pp.187-190.
- Leung C.F., Chow Y.K. and Shen R.F. (2000), 'Behaviour of pile subjected to excavation-induced soil movement', Journal of Geotechnical and Geoenvironmental Engineering, ASCE, Vol. 126, No.11, pp. 947-954.
- Meguid M.A. and Mattar J. (2009), 'Investigation of tunnel-soil-pile interaction in cohesive soils', Journal of Geotechnical and Geoenvironmental Engineering, ASCE, Vol. 135, No.7, pp. 973-979.
- Min Y., Qing S., Wei-Chao L. and Kang M. (2011), 'Three-dimensional finite element analysis on effects of tunnel construction on nearby pile foundation', Journal for central south university and Technology, Vol.18, No.3, pp. 909-916.
- Poulos H.G. and Chen L.T., (1997), 'Pile response due to excavation-induced lateral soil movements', Journal of Geotechnical and Geoenvironmental Engineering, ASCE, Vol. 123, No.2, pp. 94-99.

STRENGTH CHARACTERISTICS OF HOLLOW CONCRETE BLOCKS

V. Sivakumar*

*Assistant Professor, Department of Civil Engineering, New Prince Shri Bhavani College of Engineering and Technology, Chennai - 600073

ABSTRACT

Hollow concrete block" have become a regular or frequent choice today in construction activities as these blocks offer various benefits, simplicities in their use as building elements, strength comparable with the conventional blocks like bricks, facilities to get reinforced thereby increasing the strength of constructed units, facility for better finish, adoptability for getting desired architectural shapes and beauty and above all rendering economy in construction. With these aspect under study the authors concentrated upon some case studies indicating the uses of HCBs in the construction of beam, walls etc. to study the outcomes of these studies and have, then based on the investigations of these case studies reviewed the various aspect related to the uses of HCBs. The paper briefly reviews all the above points referred.

Keywords: Block masonry, compressive strength, economy, hollow concrete block and insulation, strength of masonry.

INTRODUCTION

One of the basic requirements of human being to sustain in the world is shelter. After evolution of human being, the need of shelter meant for safety, arises. In ancient time, man started taking shelter in caves, excavated below ground level and under hanging mountain cliffs and this type of shelter just provided safe place from environmental extremities. The concept of stability and safety as per structural features of shelter were completely out of mind. With the development and maturity of human mind, man began to modify the structural formation of shelter so as to address the increasing needs and facilities which an optimum shelter design possessed. After achieving a feat by the use of easily available material like mud in construction walls and then the technique of burnt clay brick masonry to form structural part of shelter, there was still a long journey is coming out for the best possible material for construction of stable and safe structural units of shelter. The desire for search of safe and stable structural materials keeping in view the economy of whole structure, paved way for usage of hollow concrete blocks. Now a days, Hollow Concrete Blocks (HCB) and bricks are becoming very popular. These blocks are being widely used in construction of residential buildings, factories and multi-storied buildings. These hollow blocks are commonly used in compound walls due to their low cost. These hollow blocks are more useful due to their lightweight and ease of ventilation. The blocks and bricks are made out of mixture of cement, sand and stone chips. Hollow blocks construction provides facilities for concealing electrical conduit, water and soil pipes. It saves cement in masonry work, bringing down cost of construction considerably. Economy of the structure is one of the basic aspects upon which any design is based. The stability plays an important role but the best designer is one who comes out with design which gives the stable and economics structure. The development of

the construction technology is closely related to development of adequate mechanization and handling technology. Hollow concrete is an important addition to the types of masonry units available to the builders and its use for masonry is constantly increasing.

BACKGROUND

A Hollow concrete block is primarily used as a building material in the construction of walls. It is sometimes called a concrete masonry unit (CMU). A concrete block is one of several precast concrete products used in construction. The term precast refers to the fact that the blocks are formed and hardened before they are brought to the job site. Most concrete blocks have one or more hollow cavities, and their sides may be cast smooth or with a design. In use, concrete blocks are stacked one at a time and held together with fresh concrete mortar to form the desired length and height of the wall. Concrete mortar was used by the Romans as early as 200 B.C. to bind shaped stones together in the construction of buildings. During the reign of the Roman emperor Caligula, in 37-41 A.D., small blocks of precast concrete were used as a construction material in the region around present-day Naples, in Italy. Much of the concrete technology developed by the Romans was lost after the fall of the Roman Empire in the fifth century. It was not until 1824 that the English stonemason Joseph Aspdin developed Portland cement, which became one of the key components of modern concrete. The first hollow concrete block was designed in 1890 by Harmon S. Palmer in the United States. After 10 years of experimenting, Palmer patented the design in1900. Palmer's blocks were 8 in (20.3 cm) by 10 in (25.4 cm) by 30 in (76.2 cm), and they were so heavy they had to be lifted into place with a small crane. By 1905, an estimated 1,500 companies were manufacturing concrete blocks in the United States. These early blocks were usually cast by hand, and the average output was about 10 blocks per person per hour. Today, concrete block manufacturing is a highly automated process that can produce up to 2,000 blocks per hour. Concrete blocks were first used in the United States as a substitute for stone or wood in the building of homes. The earliest known example of a house built in this country entirely of concrete block was in 1837 on Staten Island, New York. The homes built of concrete blocks showed a creative use of common inexpensive materials made to look like the more expensive and traditional wood-framed stone masonry building. This new type of construction became a popular form of house building in the early 1900s through the 1920s. House styles, often referred to as "modern" at the time, ranged from Tudor to Foursquare, Colonial Revival to Bungalow. While many houses used the concrete blocks as the structure as well as the outer wall surface, other houses used stucco or other coatings over the block structure. Hundreds of thousands of these houses were built especially in the Midwestern states, probably because the raw materials needed to make concrete blocks were in abundant supply in sand banks and gravel pits throughout this region. The concrete blocks were made with face designs to simulate stone textures: rock-faced, granite-faced, or rusticated. At first, considering an experimental material, houses built of concrete blocks were advertised in man Portland cement manufacturers' catalogs as "fireproof, vermin proof, and weatherproof" and as an inexpensive replacement for the ever-scarcer supply of wood. Many other types of buildings

such as garages, silos, and post offices were built and continued to be built today using this construction method because of these qualities.

THE BENEFITS OF HOLLOW CONCRETE BLOCK

1. Economy in design of sub-structure due to reduction of loads.
2. Saving in mortar for lying of blocks as compared to ordinary brick work. Saving in mortar for plasterwork. Uniform Plaster thickness of 12 mm can be maintained due to precision of the size of blocks as compared to brick work where plaster thickness of average 20 mm Is required to produce uniform and even plastered surface due to variations in the sizes of bricks.
3. Insulation of walls is achieved due to cavity, which provides energy saving for all times. Similarly hollowness results in sound insulation.
4. Paint on finished walls can be applied due to cavity, which provides energy saving for all times. Similarly hollowness results in sound insulation.
5. No problem of the appearance of salts. Hence, great saving in the maintenance of final finishes to the walls.
6. Laying of Blocks is much quicker as compared to brickwork hence saving in time.
7. Thermal insulation property of hollow concrete block is more than ordinary brick wall.
8. Hollow concrete block is environmentally eco friendly.
9. Factor of safety of hollow concrete block is more than brick masonry.
10. Maintenance cost of the hollow concrete block is less than brick masonry.

HOLLOW CONCRETE BLOCKS USED IN CONSTRUCTION

As regards to the use of hollow concrete blocks there are certain remarkable and noteworthy points going in favor of these blocks.
1. The dead load of hollow concrete block is much lesser than a solid block; due to this, one can work with the structural engineer and reduce steel consumption in construction.

2. Hollow concrete blocks require minimal mortar.

3. If these blocks are engineered properly then dimensional accuracy and high finishing quality is obtained.

4. Usage of lintel blocks brings tremendous operational efficiencies resulting in lower cost.

5. Hollow concrete blocks have additives to improve their water resistance and seepage minimization.

6. Hollow concrete blocks can be engineered to achieve very high compressive strengths.

7. Hollow concrete blocks are much more sturdy.

8. The hollow concrete block adopt to modern design forms, richness of the texture etc.

9. Minimum maintenance cost and cost competitiveness with other materials make it a preferred material for today's building.

10. Hollow concrete blocks can effectively be used for cold storage and industrial go downs as they are thermally effective.

Table showing description of beams:

Each beam consists of two courses of grouted of grouted hollow block masonry. All beams were singly reinforced. The reinforcement descriptions in various beams have also been shown.

Sr. No.	Designation	Dimension of beam (b x d) (mm x mm)	Longitudinal reinforcement	Shear stirrups
1.	B1	140 x 320	2- Ø8	2 lgd-Ø6 @200 c/c
2.	B2	140 x 320	2- Ø10	2 lgd-Ø6 @200 c/c
3.	B3	140 x 320	2- Ø12	2 lgd-Ø6 @200 c/c
4.	B4	140 x 305	2- Ø10	2 lgd-Ø6 @200 c/c

- Overall dimension of each beam = 140 x 390 mm
- Holding bars in each beam = 2 nos. 8 mm Ø

Construction of Beams:

Constructions of beams were done polythene sheets spread on the floor. Lower course of beam was constructed with block type "B" (channel shaped) which enables easy placing of reinforcement. Mortar mix used for assembling block was having proportion 1:3. Reinforcement cage was prepared by testing the longitudinal reinforcement with shear stirrups. This cage was

then placed in the lower course of beam. After placing reinforcement, upper course of beam was constructed using block type "C". After bars were placed in position at top of upper course of blocks by inserting them in shear stirrups. Grout of proportion 1:2.5:3 was then filled in cavities of two courses of blocks and compacted.

Testing of Beams

For testing beams, special setup was prepared between plates compression testing machine.Since the test span of beam was more than the length of trolley of machine, beams were tested upside down i.e. compression face of beam was placed at bottom and rollers of lower trolley were used as means of applying concentrated load. Load was gradually applied to the beam. On appearance of initial crack, reading of load indicating dial was taken. Then, loading was continued till ultimate failure of beam occurred.

Designation	**Dimension of beam (b x d) (mm x mm)**	**Percentage tensile reinforcement**	**Initial load (in tonne)**	**Failure load (in tonne) (W)***	**Ultimate moment (M) (in KN-m)**
B1	140 x 320	0.22	3.00	3.3	17.82
B2	140 x 320	0.35	3.40	3.6	19.44
B3	140 x 320	0.50	3.85	4.0	21.60
B4	140 x 305	0.74	4.15	4.5	24.30

W is the concentrated load at each third point of beam.

Failure Pattern and Causes of Failure

In beams, cracks initiated at middle third portion of beam where bending moment was maximum. Cracks appeared at tensile face of beam and started propagating towards compressive face with the gradual increase of load. Almost all cracks appeared at mortar a joint which happens to be weakest portion of masonry beams. At ultimate load, reinforcement started to yield which caused mortar joint to open and hence cracks appeared at mortar joint. In the experiment 4 beams were tested namely B1, B2, B3& B4 as shown in the table above. In beams B1 to B3, only flexural cracks appeared at middle third portion of beam while on beam B4, shear cracks also developed along with flexural crack. Shear cracks initiated from support and propagate

diagonally. It indicates that shear reinforcement was insufficient in beam B4. From the results of the experimental study conclusions that can be drawn are:

- The order to use HCBs in making a beam, percentage tensile reinforcement in blocks should be adequate so as to increase moment carrying capacity of beam.
- The beams so created using HCBs should be never are left under reinforced so as to stop the initiation of the cracks from bottom face of the beams.
- Utmost care should be taken to see that the mortar joints in the masonry made of HCBs does not happen to be the weakest portion for the initiation of the cracks.
- All possible care should be exercised to see that the beam safe in shear and diagonal cracks do not take place at supports.

Discussion on wall

Three sets of wall of size 0.2m width, 0.8m length and 1.8m height constructed with different mortar 1:3, 1:4, 1:5 proportion were tested in the compression testing machine (CTM). Each set consist of three wall made up of same proportion of mortar. Because of the concrete of being homogenous, the structure gives different results when tested under the same conditions. The walls were kept hollow inside. The load carrying capacity of the walls and the crack patterns developed due to the load were studied. The HCBs tested in CTM. The bearing surfaces of the CTM are wiped clean and any dry loose or other materials are removed. The HCBs taken out from the curing and are allowed drying for 24 hours in open air. The dimensions of the HCBs are measured to the nearest 0.2 mm and their weights are noted before testing. The load is applied in these bed faces. The axis of the bed face is carefully aligned with the center of spherical seated plate. No packing is used the faces of the test specimen and steel plate of the testing machine. Compressive strength of the HCB tested in CTM is as shown in the table below.

Sr. no.	Size of hollow concrete block	Average compressive load of 10 reading	Stress in N/mm^2 on net area
1	400X200X200	9.0	2.2
2	200X200X200	10.0	8.8

During the experiment for wall of size 0.2m x0.8m x1.8m, the concrete plate was cast of size 0.4mx1.0mx0.1 m also hooks were made for putting the edge of bars of the steel provided in mesh of the concrete plate. For column size 0.4mx0.4mx1.8 m, the concrete plate was cast of dimension 0.6m x0.6m x0.1 m. This plates were cast simultaneously and allowed curing for 28 days to got the enough strength of plates. After that the walls were constructed on it.

Wall Test

Compressive test of the nine walls with different mortar proportion was carried out and the results are shown in following tables.

Wall constructed with mortar 1: 5

Sr. no.	Load at initial cracks in tone	Load at final cracks in tone	Stress at initial cracks in N/mm²	Stress at final cracks in N/mm²
1	12	12.5	1.46	1.52
2	11.6	12.8	1.41	1.56
3	11.7	12.3	1.43	1.50

Wall constructed with mortar 1: 4

Sr. no.	Load at initial cracks in tone	Load at final cracks in tone	Stress at initial cracks in N/mm²	Stress at final cracks in N/mm²
1	11	12	1.34	1.46
2	10	12	1.22	1.46
3	10	13	1.22	1.49

Wall constructed with mortar 1: 3

Sr. no.	Load at initial cracks in tone	Load at final cracks in tone	Stress at initial cracks in N/mm²	Stress at final cracks in N/mm²
1	6.5	7.0	0.79	0.85
2	11.5	12.4	1.4	1.51
3	12.5	13.5	1.52	1.65

The only conclusion that can be drawn, form these case study is, that the wall constructed using HCBs is more economical than the brick wall and renders speedy construction.

CASE STUDY III: BRICK MASONRY AND HOLLOW CONCRETE BLOCK-A COMPARISION

In two case studies indicated above the structures created using HCBs were tested for specific purpose namely for flexural strength, in case of beam, and load carrying capacity in case of wall, Unlike these two case studies one study was carried out by Rafiq Ahmad et.al to compare brick masonry and HCB masonry. The study was carried out concentrating upon cost aspect. The various constituents of the entire study are discussed below:

Testing:-

1. Testing of individual hollow concrete block and brick units:

Individual hollow concrete blocks confining to IS: 2185-1984 (Part 3) and brick units confining to IS : 1077-1986, IS : 2180-1985 and IS : 2222-1979

2. Testing of mortar blocks of size (15x15)cm were made and tested after 28 days confirming with IS: 4031 (part 1).

3. Testing of wall: After the walls were built curing was done for 7 days and testing was done after 28 days. A rail section which completely covered the top section of the wall was placed. The rail section was placed so that load from the jack would be uniformly distributed over the wall. The jack was placed centrally over the rail fixed to the upper member of the frame. The proving ring was placed under the jack for measurement of the load. The testing was started by pumping the jack at a higher rate initially then lowering the rate as cracks appeared, in order to observe the modes of failure.

CONCLUSION

The main aim of the paper being the review of the experiences obtained by different researchers in their studies to use the HCBs for constructing various structural elements, three case studies have been indicated above. Based on the observations discussed in these case studies the authors would like to draw the following conclusions:

1. Being light in weight HCBs provide economy in design of sub-structure due to reduction of the loads.
2. Laying of blocks saves mortar as compared with ordinary brick work. There is saving in mortar plaster work too.
3. Cavity of blocks helps achieving insulation of walls and provides energy saving for all times. Hollowness results in sound insulation.

In view of all the above discussions and the conclusions drawn thereafter, it can be finally concluded that if the HCBs are engineered properly then they help obtaining dimensional accuracy and high finishing quality and having cost competitiveness with other materials they have become the preferred materials for today's buildings.

REFERENCES

ACI Committee 531, "Building code Requirements for Concrete Masonry Structures", ACI Jounral, Proceedings V.75, No.8, p. 384-403, Aug. 1978.

ACI Committee 531, "Commentary on Building Code Requirements for Concrete Masonry Structures", ACI Jounral, Proceedings V.75, No.8, p. 460-498, Sept. 1978.

Boult, B. F., "Concrete Masonry prism testing", ACI Jounral, Vol.76, p. 1145, Oct. 1979.

Curtin, W. G., Shaw, G. and Beck, J. K. "Design of reinforced and prestressed masonry", Granada publishing limited, London, 1988.

Curtin, W. G., Shaw, G., Beck, J. K. and Parkinson, G. I., "Structural Masonry Detailing", Granada Publishing Limited, London, 1989.

CYBER CRIMES BECOMING THREAT TO CYBER SECURITY

Kavitha.P
Department of Computer Science &Engg, New Prince Shri Bhavani College of Engineering and Technology , Gowrivakkam , Chennai-73.
E-mail: kavitha@newprinceshribhavanil.com

Anitha.S
Department of Computer Science &Engg, New Prince Shri Bhavani College of Engineering and Technology **,** Gowrivakkam , Chennai-73.
E-mail:anitha.s@newprinceshribhavani.com

ABSTRACT:

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. The growing danger from crimes committed against computers, or against information on computers by persons involved in the profession of crimes, has become a major issue in India. For an effective application, the existing laws must be constantly reviewed and modified accordingly to face the challenges coming from the cyber world. In this paper, we've discussed the cyber crimes as one of the challenges for cyber laws and it also discussed about the cyber crimes that have continued to grow as one of the threats to the users of the cyber society. We've also discussed the laws in cyber space and their need along with the IT Act-2000. Some more viewpoints presented in the paper include: the legal drawbacks with regards to cyber crimes being solved in India, and the need for new legalizations. The main emphasis of the paper revolves around the challenges faced by cyber laws in regulating cyber crimes.

Keywords : Cyber crimes, cyber laws, cyber society.

INTRODUCTION

The rapid change occurring in the present era of information technology includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element. Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and different activities [1]. Cyber laws help in maintaining a trustworthy environment for cyber society by applying rules of law in criminal investigations. Cyber crime is a criminal activity committed on the internet and is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce
sites to lose money. Cyber laws are meant to set some rules and guidelines that make the cyber activities legalized. One of the major challenges laws have been facing has been in the cyber space crimes as cyber technology changes have been so rapid that it has become a difficult issue for law enforcement agencies to keep up with this rapid change.

CYBERCRIMES IN CYBER SPACE

The growing danger from crimes committed against computers, or against information on computers, has become a major issue in the India. Cyber crime is a broad term that describes everything from electronic cracking to denial of service attacks that cause ecommerce sites to lose money. The Encyclopedia Britannica defines cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology [2]. Cyber crimes are harmful acts committed from or against a computer or network. Some other cyber crimes include:

 Using one's own programming abilities as also various programs with malicious intent to gain unauthorized access to a computer or network are very serious crimes.

 Creation and dissemination of harmful computer program which do irreparable damage to computer systems is another kind of cyber crime.

 Software piracy is also another distinct kind of cyber crime in which many people online distribute illegal and unauthorized pirated copies of software. Indian Penal Code does not use the term „cyber crime' at any point even after its amendment by the IT Act 2000.

Cyber crimes in the cyber society can be basically divided into 3 major categories [3]:
2.1. Cyber crime against Persons
2.2. Cyber Crimes against Property
2.3. Cyber Crimes against Government

2.1. Cyber crime against Persons

Cyber crimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer like e - mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important cyber crimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one cyber crime which threatens the growth of the younger generation. Harassment can be sexual, racial, religious, or other and persons perpetuating such harassment are also guilty of cyber crimes.

2.2. Cyber Crimes against Property

The second category of cyber-crimes is that of cyber crimes against all forms of property. These crimes include computer vandalism i.e. destruction of others' property, and transmission of harmful program.

2.3. Cyber Crimes against Government

The third category of cyber-crimes relate to cyber crimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the international governments and also to terrorize the citizens of a country. Cyber crime occurs when an individual "cracks" into a government or military maintained website. During the investigation of the Red Fort shootout in Dec. 2000, the accused Ashfaq Ahmed of this terrorist group revealed that the militants are

making extensive use of the internet to communicate with the operatives and the sympathizers and also using the medium for intra-bank transfer of funds" [3].

NEED FOR CYBER LAWS AGAINST CYBER CRIME

It is common that many systems operators do not share information when they are victimized by crackers. They don't contact law enforcement officers when their computer systems are invaded, instead prefer to fix the
damage and take action to keep crackers from gaining access again. Computer crime poses a real threat and as the cases of cyber crime grow, there is a growing need to prevent them. Cyberspace belongs to everyone; so there should be some kind of electronic surveillance i.e.investigators to track down/ monitor the hacker/cracker as he breaks into a victim's computer system. The basic laws governing real-time electronic surveillance in criminal investigations must also apply in this context like the search warrants to be obtained to gain access to the premises where the cracker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime. To overcome the security flaws, we‟ve some suggestions for cyber society [4]:

• Protect your databases and place the database behind a second interface on your firewall, with tight access rules.

• Avoid giving out any information about yourself in a chat room. Children should never arrange face-to-face meetings or send their photographs online.

• Use the latest anti-virus software, operating systems, web browsers and email programs and put in a firewall and develop your content off line. Use a security program that gives you control over cookies that send information back to Web sites.

• Make sure web servers running your public site are physically separate and individually protected from your internal corporate network. Send credit card information only to secure sites.

• Back up your web site after every update, so you can relaunch it immediately in case of a malicious defacement. Internet provides anonymity: this is one of the reasons why criminals try to get away easily when caught and also give them a chance to commit the crime again. Therefore, we users should be careful and if we find anything suspicious in e-mails or if the system is hacked, it should be immediately reported to the police officials who investigate cyber-crimes rather than trying to fix the problem by ourselves.

TECHNOLOGY CHALLENGES IN CYBER CRIME

In the present era of advancements in technology, law enforcement agencies must provide their computer crime investigators with the technology required to conduct complex computer investigations. Besides access to technology, law enforcement agencies must also be given Forensic Computer support as many computer crimes leave “footprints” on the computer as well as on the internet [5]. Most of the prosecutors also lack the specialization to focus on the prosecution of criminals who use computer-based and Internet system as a means of committing crimes. Moreover, the prosecutors must have enough knowledge of computer-based and Internet investigations if they have to handle these crimes effectively. Law enforcement must seek ways

to keep the drawbacks from overshadowing the computer age. Cyber crimes have to be tackled effectively not only by the law officials but also by the cyber society by co-operating with the law.

THE IT ACT 2000: THE FIRST CYBER LAW

The Parliament of India passed its first Cyber law, the Information Technology Act in 2000 i.e. IT Act-2000. It not only provides the legal infrastructure for Ecommerce in India but also at the same time, gives powers to the police to enter and search, without any warrant, any public place for the purpose of nabbing cyber-criminals and preventing cyber crime [7]. The IT Act 2000 gives the legal framework so that information is not denied legal effect, solely on the ground that it is in the form of electronic records. In fact, the Indian Penal Code does not use the term „cyber crime' at any point even after its amendment by the IT Act 2000. On the contrary, it has a separate chapter XI entitled “Offences” in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine. The offences covered under Chapter XI of the Indian Information Technology Act 2000 include [6]:
(i) Tampering with the computer source code or computer source documents
(ii) Hacking

(iii) Publishing or transmitting any information in the electronic form which is lascivious or which appeals to the prurient interest.

(iv) Failure to decrypt information if it‟s necessary in the interest of the sovereignty or integrity of India.

(v) Securing access or attempting to secure access to a protected system.

(vi) Mis -Representation while obtaining, any license to act as a Certifying Authority or a digital signature certificate.

(vii) Breach of confidentiality and privacy

(viii) Publication of digital signature certificates which are false in certain particulars

(ix) Publication of digital signature certificates for fraudulent purposes.

DRAWBACKS OF CYBER LAWS AGAINST CYBER CRIMES

Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space. India is the 12th nation in the world that has cyber legislation. The cyber
laws of the country could not be regarded as sufficient and secure enough to provide a strong platform to the country‟s e-commerce industry for which they were meant [7]. However, it is important to note that existing laws do not help in solving cyber crimes efficiently. There are many drawbacks which prevent cyber crimes from being solved in India:

 Most people in India prefer not to report cyber crimes to the law enforcement agencies because they fear it might invite a lot of harassment.

 Awareness of cyber crime is extremely low. Awareness of people about cyber crime is still very low and so we need to take many steps to alert the legal scenario.

 Law enforcement agencies in the country are not well equipped and knowledgeable enough about cyber crime.
 An immense need for training the law enforcement agencies: very few cities have cyber crime cells viz. under the IT Act, the relevant officer entitled to investigate a cyber crime is a Deputy Superintendent of Police (DSP), but most of the DSP‟s are not well equipped to fight cyber crime.

 There is also a lack of dedicated cyber crime courts in the country where expertise in cyber crime can be utilized.

 The Law enforcement agencies have been facing tremendous problems while trying to cope with the challenges of emerging cyber crimes.

IMPROVEMENTS REQUIRED IN CYBER LAWS

The law enforcement agencies have been facing tremendous problems while trying to cope with the challenges of emerging cyber crime within the ambit of the Indian Penal Code [8], even if a liberal interpretation of it is taken. As far as the issue of solving cyber crime goes, the credit lies with the law enforcement agencies. There is a need for some new and distinct laws on cyber crime and appropriate changes should also be made in the Indian Penal Code and the IT Act. However, cyber law is indeed helpful in addressing some cyber crimes but in the areas where the law does not cover cyber crimes which have already emerged, the law is of no assistance or help whatsoever. Moreover, there is a need for dedicated, continuous, updated training of the law enforcement agencies. While Indian laws are well-intentioned, there is a general perception among the population that one can get away with any crime due to various flaws in the execution. It is important to know that existing laws are not well equipped enough to deal with cyber crimes as they do not possess the latest tools. People need to be encouraged to report the matter to the law enforcement agencies with full confidence and trust and without the fear of being harassed. Further, the law enforcement agencies dealing with cyber crime need to come up with an extremely friendly image.

CONCLUSION

Cyber crime that has become a great threat to the cyber society, has to be tackled efficiently not only by the law officials but also by the cyber society. The IT Act 2000 has developed great assistance to the cyber law prosecutors to put the cyber criminals behind the bars.

Being co-operative with the law, the problem could be solved to a great extent i.e. if the law enforcement agencies dealing with cyber crimes have been extremely cooperative with cyber society. To conclude, in order to deal with the problem of cyber crimes along with better legal implementations, a need for some new laws along with a pro-active approach by the law enforcement agencies still exists.

REFERENCES

[1] Latika Kharb, Balwant Rai, Pradeep Tomar, “New Vision of Computer Forensic Science: Need of Cyber Crime Law”, The Internet Journal of Law, Healthcare and Ethics, 2007. Volume 4, Number 2. ISSN: 1528-8250.
[2] Curtis P A., Cowell L. ” Cyber Crime”: “The Next Challenge” in seminar at School of Law Enforcement Supervision in November 12, 2000

[3] Maya Babu, Mysore Grahakara Parishat, ”What Is Cybercrime”, in Star Of Mysore, Online magazine, October 11, 2004

[4] Gopika Vaidya-Kapoor , “Byte by Byte” in Net Guide, Online magazine, February 18, 2003

[5] National ICT Security and Emergency Response Centre (NISER) “Is Cyber Crime reigning on a no Man‟s land”.

[6] www. economictimes.indiatimes.com

[7] Vijayashankar N. “The role of Cyber Laws in EGovernance” Paper presented at the Seminar in Chennai
on September 16, 2000

[8] www.cyberlaws.org

DRIVING WITH SHARKS: RETHINKING CONNECTED VEHICLES WITH VEHICLE CYBER SECURITY

Anitha.S
Department of Computer Science & Engg, New Prince Shri Bhavani College of Engineering and Technology **,** Gowrivakkam , Chennai-73.
E-mail:anitha.s@newprinceshribhavani.com

Kavitha.P
Department of Computer Science & Engg, New Prince Shri Bhavani College of Engineering and Technology , Gowrivakkam , Chennai-73.
E-mail: kavitha@newprinceshribhavanil.com

ABSTRACT:

In a public service announcement on March 17, 2016, the Federal Bureau of Investigation (FBI) jointly with the Department of Transportation and the National Highway Traffic Safety Administration released a warning over the increasingvulnerability of motor vehicles to remote exploits1. Engine shutdown, disable brakes and door locks are few examples of the possible vehicle cyber security attacks. Modern cars grow into a new target for cyberattacks as they become increasingly connected. While driving on the road, sharks (i.e., hackers) only need to be within communication range of your vehicle to attack it. However, in some cases, they can hack into it while they are miles away. In this article, we aim to illuminate the latest vehicle cyber security threats including malware attacks, On-Board Diagnostic (OBD) vulnerabilities, and auto mobile apps threats. We illustrate the In-Vehicle network architecture and demonstrate the latest defending mechanisms that are designed to mitigate such threats.

INTRODUCTION

Nowadays, vehicles are no longer isolated mechanical machines that are solely used for transportation. Consumers are increasingly demanding a seamless connected experience in all aspects of their lives including driving. With the introduction of telematics, vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications, and the integration of smart phones and Bluetooth devices, connected vehicles represent an eco-system that is part of a fully connected world. In fact, connected vehicles are an integral part of the smart city vision and a node in the world of Internet of Things (IoT). On the other side, vehicles themselves are now controlled by hundreds of Electrical Control Units (ECUs) that form an internal network of devices within the vehicle. While increasing autonomy and connectivity in vehicles bring many improvements in terms of functionality and convenience, it also brings a new cyber threat plane into life where vehicles become a new target for attackers/hackers [1].

As software starts to permeate more functions in the modern vehicles that are Internet connected, we propose to play the following game of words: 1) If you see the word “software”, replace it with “hackable”; and 2) If you see the word “connected”, replace it with “exposed”. As it stands, you can imagine that while driving your “hackable exposed” modern car, you are surrounded by sharks. These sharks try to attack and/or hack into your vehicle and may cause a real damage that cannot be recovered. Since it is a life-threatening issue (i.e., considered as a

lethal cyberattack), in April 2016, the Michigan state Senate has proposed two bills that introduce life sentences in prison for people who hack into vehicles' electronic systems [2].

Figure 1 Hackers remotely kill a Cherokee Jeep on highway with the driver in it using a simple 3G connection [3]

Figure 1 shows an example of a demonstrated cyber security attack against a Cherokee Jeep car on a highway, also known as cyber carjacking. In July 2015, two researchers Charlie Miller and Chris Valasek hacked into the Cherokee Jeep from Miller's basement while the car itself was placed on the highway ten miles away [3]. They were able to remotely control the car functions using a simple 3G connection exploiting a vulnerability in the Uconnect software. Uconnect is Internet connected software that controls the navigation and the entertainment system in the vehicle. Through the discovered Uconnect's cellular vulnerability, which represents the attacking entry point, they had the ability to rewrite the firmware of the adjacent chip in the car's head unit. Consequently, they sent commands through the In-vehicle network, which is illustrated in the next section, to disable the brakes and take control over the steer wheel, and finally sent it to a ditch as showed in Figure 1. This cyber carjacking incident caused the recall of 1.4 million cars.

In fact, it is not only the problem of Chrysler vehicles with Uconnect software. There are other attacks that have been recently reported against other manufacturers' vehicles. Examples of the most recent reported attacks are:
Last summer, June 2016, the Mitsubishi Outlander Plug in Hybrid Electric Vehicle (PHEV) was hacked. Security researchers at Pentest Partners [4] performed a man in the middle attack between the PHEV's mobile app and the PHEV's Wi-Fi Access Point (AP). After replaying various messages from the mobile app, they figured out the binary protocol used for messaging. Consequently, they were able to turn the lights on and off and disable the whole theft alarm system leaving the vehicle vulnerable to more attacks.

• Garcia et al. [5] showed that almost 100 million Volkswagen vehicles sold between 1995 and 2016 are vulnerable to remote keyless entry hacks. Volkswagen vehicles depend on few global master keys that can be
recovered from ECUs. This way, the attacker can clone a Volkswagen Group remote control and, by eavesdropping on a single signal sent by the original remote, he/she can gain unauthorised access to the vehicle.

• Through a vulnerability in NissanConnect mobile application, which controls Nissan Leaf electric vehicle, attackers took control over the heater in the car and turned it on all the time to drain the battery. This incident forced Nissan to disable that application [6].
• An attacker within the SmartGate in-car Wi-Fi range of the SmartGate-enabled Škoda car can steal information about the car [7]. Moreover, he/she can lock out the car's owner
from the SmartGate system.

• Finally, using a laser pointer and a Raspberry PI, Jonathan Petit, a security researcher, was able to interfere with the laser ranging (LIDAR) systems of the self-driving car to trick it into thinking that there are obstacles (i.e., other cars or pedestrians) ahead of it [8]. This trick can bring a selfdriving car at full speed to stop thus, disabling the car. Selfdriving cars depend on LIDAR systems, which create a 3D map, to navigate and see if there is any potential hazard or obstacle as can be seen in Figure 2. Petit simply fired his laser pointer, which is pulsed by the Raspberry PI, at the self-driving car. When it is picked up, the LIDAR unit is tricked into seeing illusory objects when turning right.
Consequently, the car stopped at once. This attack worked up to 100m away in any direction and did not require a tightly focused beam.

Hence, physical access to the car is no longer a precondition to hack into it. Sharks on the road only need to be in communication range of the targeted vehicle (e.g., its Wi-Fi range) to gain important information and even take control of the vehicle's most critical functions. However, in some cases like in the Uconnect software attack, the sharks can be miles away from the targeted vehicle. Besides taking over control of the steer wheel and disabling brakes, a simple and sudden airbags deployment while driving on a highway represents a lethal cyberattack that could cause the vehicle to crash and costs lives.

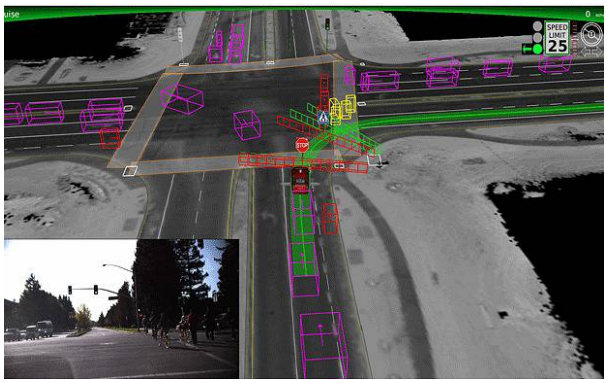

Figure 2 What a self-driving car sees when turning right [8]

In practice, besides recalling the vulnerable cars and offering Over-The-Air (OTA) updates, the auto industry should respond in a better way to avoid embarrassing hacks and costly recalls. The last reported incidents were the motive for a series of events that brought together many car manufacturers along with law agencies and governmental bodies (e.g., see [9]). The aim of these events was to put an effective strategy to share information, raise threat awareness across the auto industry, listen to consumers' concerns about security and privacy, learn about the required legalisations, and put vehicle IT at the centre of the development process. Yet, more efforts are needed to address vehicle cyber security concerns.

In-Vehicle Network Architecture (Automotive Network)

To develop an understanding of the potential entry points (i.e., attacking points) the hackers can expose in the modern car, in this section, we illustrate the In-vehicle network architecture, also known as the automotive network, in detail. Modern cars contain between 30 to 100 ECUs, which are embedded computers that communicate among each other creating the In-vehicle network [10]. ECUs' intercommunication is essential to efficiently monitor and configure
different vehicular subsystems. Figure. 3 shows that the In-vehicle network is composed of many electronic subsystems including embedded telematics, body and comfort control, vehicle safety, power train, on-board video cameras and In-Vehicle Infotainment (IVI) [11]. Each subsystem contains many ECUs each of which controls a specific functionality in the vehicle. For instance, ECUs that control airbags deployment and Antilock Braking System (ABS) are found in the vehicle safety subsystem, while ECUs that provide engine control and suspension control are found in the power train subsystem.

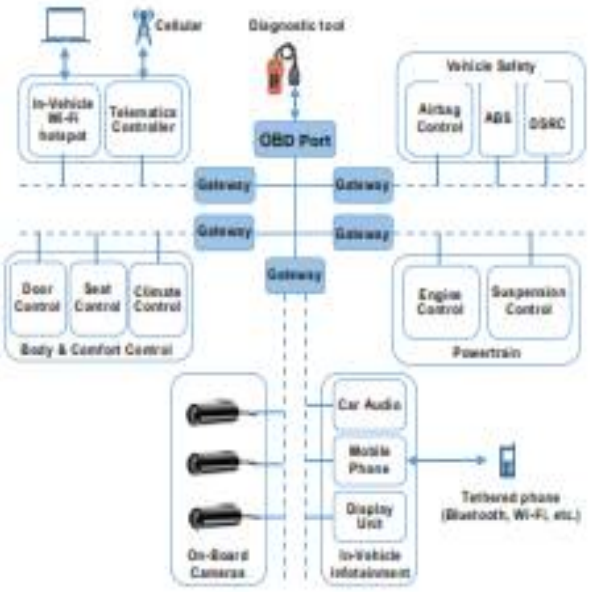

Figure 3 In-Vehicle (Automotive) Network Architecture [11]

To guarantee the desired functionality and on-time response to critical events, ECUs of the same or different subsystems need to communicate among each other. Based on the time-sensitivity of the provided functionality, different In-vehicle sub-networks are utilised. For instance, high-speed Control Area Network (CAN) is used for time-critical engine control, safety subsystems, and powertrain, while for less time-sensitive body
and comfort control subsystem a Local Interconnect Network (LIN) is used [11]. To support audio, video and on-board cameras, Media-Oriented Systems Transport (MOST) and Ethernet are employed in the IVI subsystem. These networks are interconnected through gateways that control messages flow
among the subsystems as showed in Figure. 3. At the same time, these gateways are interconnected through a high-speed CAN buses.

Given the recent trends of connecting different devices through USB, Bluetooth, Wi-Fi, 3G/4G etc., each In-vehicle network subsystem implements its own communication module to

connect to the outside world. For instance, IVI allows both wireless communication through Bluetooth and wired
communication through USB. Cellular communication is implemented in the embedded telematics subsystem that can offer a Wi-Fi AP. Moreover, modern vehicles are now fitted with On-Board Diagnostic (OBD) ports that are utilized for vehicle inspection, ECU firmware updates and repair. Furthermore, OBD port allows full access to the In-vehicle network.

Thus, the variety and the increasing number of connection points in each In-vehicle network subsystem make the vehicle more accessible from the outside world. Consequently, more vulnerable to different cyber attacks. Indeed, each communication interface with the outside world should be protected. However, protecting each entry point separately will result in duplicate securing functions on the same vehicle. Moreover, restrictions such as limited computational power and storage capabilities should be considered.

Cyber Threats Vectors against Connected Vehicles

As we have explained before, connected vehicles have a broad cyberattacks surface where attacker can gain control over the vehicle. Remote key entry, Wi-Fi, Bluetooth, Dedicated Short Range Communications (DSRC), OBD, USB, and Auto mobile apps are few examples of attacks entry points against connected vehicles as illustrated in Figure 4.

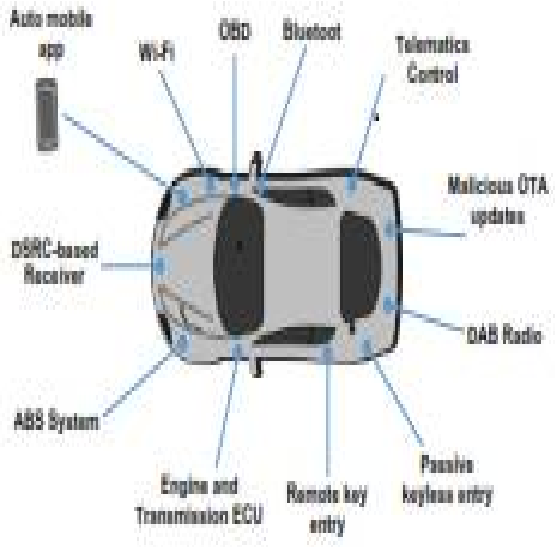

Figure 4 Connected Vehicles Security – Potential Cyber Threat Vectors

In the following, we explain four cyber threats vectors against connected vehicles: OBD threats, DSRC security issues, malware attacks, and mobile auto apps threats.

OBD Threats

The implementation of OBD is mandatory in vehicles sold in the US since 1996, in the European Union since 2001 for gasoline powered-vehicles, and for the diesel-powered ones since 2004 [10]. The OBD port is primarily used to allow cars to report any problem in its infrastructure and communicate the diagnostic data collected by its sensors to the outside world. This allows the service provider to fix the reported problems. OBD dongles are used to interface with the OBD port and consequently access the CAN network within the vehicle. These OBD dongles can be

purchased by anyone and they are fairly cheap. OBD ports are considered as entry points to attack the ECUs that are connected to the CAN buses. The authors in [12] showed how an automotive virus can be injected into the ECUs through the OBD port and trigger specific messages on the bus (e.g., door locks) when specific conditions are met.

While the above-mentioned attack in [12] requires physical access to the vehicle, modern cars now allow OBD dongles to be remotely controlled by Wi-Fi connection from a computer. In [13], vulnerabilities in the API of a pass-thru device (i.e., OBD dongle) allow the attacker to inject a malicious code into it. This malicious code makes the pass-thru device emitting malicious packets on the CAN buses every time it is plugged into a different vehicle. In a recent survey [14], over 50% of the surveyed OBD dongles, are vulnerable to hacking. Weak encryption, exposed keys, and communication hijacking are the top three security flaws in these dongles.

DSRC Security Issues

V2V and V2I communications are key technologies to offer a class of safety services for connected vehicles that can prevent collisions and save lives. DSRC technology has been developed for use in V2V and V2I communications, where each vehicle is assumed to be equipped with DSRC On-Board Unit (OBU). DSRC communications utilize several standards such as IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) for PHY and MAC functions, IEEE 1609.2 for security services, and IEEE 1609.3 for network services.

To achieve its goal, DSRC equipped vehicles are expected to communicate (i.e., send/receive/relay) information to other DSRC equipped vehicles and/or infrastructure such as Road- Side Units (RSU). This principle opens the door for malicious nodes to either hack into DSRC equipped vehicle or cause damages by sending fake safety information. Therefore, IEEE 1609.2 defines standard mechanisms to authenticate and encrypt messages in DSRC. Nevertheless, attacks such as Denial-of- Service (DoS) are still possible. In [15], Lyamin et al. investigated the jamming DoS attacks in IEEE 802.11p when a malicious node corrupts the exchanged safety messages in a platoon. Furthermore, they proposed a simple real-time detector of jamming DoS attacks in vehicular networks.

Besides jamming DoS attacks, malware, GPS spoofing, location tracking, masquerading, and black holes are few examples of threats to DSRC equipped vehicles. Hence, more research efforts in collaboration with the auto industry are needed to mitigate such attacks.

Malware Attacks

Malware can affect the connected vehicle in many ways. It can exploit known vulnerabilities in the design and implementation of In-vehicle network subsystems and components, the software update packages of ECUs, and the vulnerabilities in the operating systems used in the vehicle. The amount of malicious actions that can be performed by malware is endless. For instance, malware can disrupt the normal operation of vehicle features such as locking the in-car radio so the users cannot turn it on, cause driver distractions by arbitrarily turning on the in-car audio and tuning the volume up, disable vehicle safety functions such as the ABS, lock the vehicle’s door and request a ransom to open it, and send fake safety data to other vehicles on the road [11].

In the connected vehicle, any communication interface can be a potential entry point for a malware. This includes OBD ports, remote ECU firmware and software updates (i.e., OTA), removable media ports, and embedded web browsers. It is worth noting that more vehicles are using Linux-based operating systems, which are more resilient to malware attacks than other operating systems like Microsoft Windows and Android. However, malware attacks on Linux have been on the rise [11]. Thus, we cannot assume that connected vehicles that are using Linux are completely immune to malware threats.

Auto Mobile Apps Threats

OEM-endorsed connected car solutions such as Apple's CarPlay and Google's Android Auto interfaces will bring more integrated, but potentially vulnerable, mobile apps into the connected vehicle [14]. Vehicles vendors are offering a wide range of auto mobile apps that leverage 3G/4G connections and/or Wi-Fi to communicate with your car and run diagnostic tests. However, these apps carry a lot of risk and security vulnerabilities that can cause personal data leakage and malware infection (e.g., the NissanConnect app vulnerability explained above). Besides that, a successful attack against a downloadable auto mobile application (e.g., inject a malicious code or plant a Trojan horse) in Apple Appstore or the Google Play Store would have serious consequences on the security of the connected
vehicle, which may use that infected app.

Moreover, it is noticeable that most of the recent reported attacks against connected vehicles have been conducted through an auto mobile app vulnerability. The method the mobile app uses to connect to the car plays a crucial role deciding how secure using this app is. Most auto mobile apps that allow remote access to the car utilize a web service hosted by a service provider. This web service then connects to the car using 3G/4G mobile data connection. However, some vehicles do not use cellular connections or web services. Instead, they allow mobile apps to connect directly to the car's Wi-Fi AP and control its functions. If it is implemented poorly, this method is vulnerable to many security and privacy attacks such as geo-locating the vehicle using its AP SSID and capturing the Pre-Shared Key (PSK) between the car's Wi-Fi AP and the mobile app. Hence, gaining unauthorized access to the vehicle's functions as in the Mitsubishi Outlander PHEV hack [4], which was explained earlier.

Defending/Protection Mechanisms

While it is possible to use strong security measures and mechanisms in ordinary networks to protect it, the limited processing power of the In-vehicle network subsystems does not allow the same. Furthermore, ECUs usually come from different vendors. Thus, it is not feasible to design one security solution for the whole system. One suggestion is to isolate the In-vehicle physical network to make sure that infecting one subsystem will not affect the entire network. However, this is not feasible with the increasing need for those subsystems to communicate among each other as explained via Figure. 3.

Recently, three main approaches have emerged to protect/defend connected vehicles against cyber security threats, and respond as quickly as possible to the reported hacks. In the following, we illustrate these three approaches in detail.

OTA Solution

One of the biggest challenges that face the auto industry is to retrofit protection mechanisms in vehicles that were not secure or need to be secured against a recent threat/vulnerability.

This may include software fixes, firmware upgrades, and security patches. To address this challenge and avoid costly recalls, more vehicles' manufacturers start using the OTA updates.

While OTA updates represent a reasonable solution to respond to cyber threats in connected vehicles, it suffers a major problem. Fixing vulnerabilities using OTA updates is a security risk. When OTA is delivered to the connected vehicle, it means that a remote code is allowed to execute. Thus, if security is not well implemented around the OTA updates, it can lead to serious
consequences. Some security mechanisms such as authenticating the OTA update, use a secure protocol to deliver it, and cryptographically verify the OTA update must be in place. This is also called Secure OTA (SOTA), which has been the focus of many research efforts lately.

Cloud-based Solutions

Since it is not feasible to protect each In-vehicle subsystem individually, centralized solutions have emerged to protect the In-vehicle network and consequently the connected vehicle. For instance, Ericsson has developed a cloud-assisted solution called the Connected Vehicle Cloud (CVC) system [16]. The CVC system establishes a new channel between the vehicle and a variety of services and support provided by partners and OEM controlled partners. The security layer provided in CVC ensures that the communication between the vehicle and the system is encrypted. It also contains an anomaly detection unit to detect any malicious attempt to hack into the vehicle. Finally, through a secure gateway, CVC filters the contents of the web surfing traffic to make sure that no viruses or malwares could infect the vehicle. Figure 5 shows an overview of the CVC system.

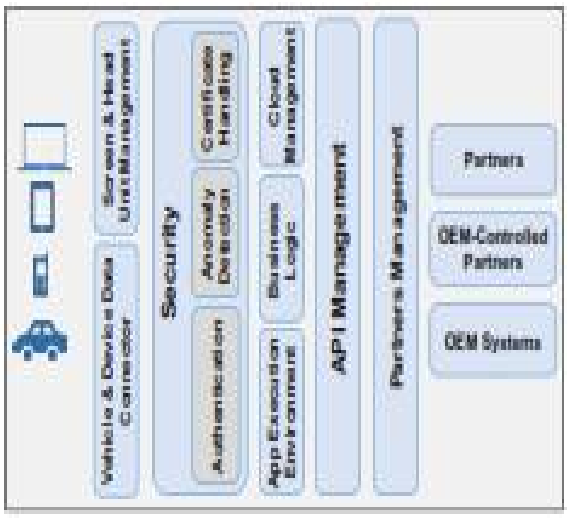

Figure 5 Ericsson Connected Vehicle Cloud Overview [16]

In [11], Zhang et al. proposed a cloud-assisted vehicle malware defence framework since it is impractical to rely on the vehicle itself to defend against malware. The authors present lightweight malware defence functions, in terms of processing power and storage, that operate in the vehicle. With the
assistance of a security cloud, the on-board malware defence functions will have full access to a wide range of malware defence mechanisms and an up-to-date large malware information database. This eliminates the limited storage problem in the In-vehicle network. It is also

suggested that the traffic can be routed through the security cloud to filter out any viruses or malware before reaching the connected vehicle as in Ericsson CVC system [16].

While the cloud-based solutions to secure connected vehicles look very promising, there are three main issues to examine. First, communications overhead and the delay incurred by routing the traffic through the cloud services need more investigation (e.g., routing V2V and V2I traffic to the cloud to defend against DSRC attacks is impractical). Secondly, these solutions heavily depend on the fact that the cloud-based systems are secure. However, if the cloud-based system is infected with a malware, it will spread to all its connected vehicles and could lead to severe damages. Finally, these solutions assumed that vehicles are connected to the cloud-based system all the time via the Internet. This may not be possible everywhere and would incur high costs for consumers.

Layer-based Solution

Finally, the National Highway Traffic Safety Administration (NHTSA) has launched a research programme that takes a layered approach to cyber security for motor vehicles [17]. According to NHTSA, this layered approach reduces the probability of attacks and mitigates the potential ramifications of a successful one. The programme focuses on four main areas at the vehicle level:

1) Preventive measures and techniques such as isolation of safety critical subsystems to mitigate the effects of a successful attack;

2) Real-time intrusion detection measures that include a continuous monitoring of potential intrusions in the system;

3) Real-time response methods that aim to preserve the driver's ability to control the vehicle when the attack is successful; and

4) Assessment of solutions where information about successful hacks from partners can be collected and analyzed to assess the effectiveness of the current protection mechanisms.

Conclusion

Vehicle cyber security is a very serious subject area that needs more investigation and research efforts from academia, auto industry and governmental bodies. Damages of automotive cyber attacks can be severe and irreversible as it concerns human lives. While manufacturers are looking to equip modern vehicles with more connectivity and smart functions, vulnerabilities are increasing rapidly. These vulnerabilities in wired and wireless communications interfaces allow sharks to hack into vehicles and take control. Some attempts to devise solutions to protect/defend connected vehicles and respond to reported hacks are very promising. However, more work and collaboration are still required to protect our connected vehicles and consequently our lives on the roads.

References

[1] S. Nathan, "Hackers after your car? Tackling automotive cyber security," The Engineer, Sept. 24, 2015

[2] S. Khandelwal, "Car Hackers Could Face Life In Prison. That's Insane!," The Hacker News, May 01, 2016.

[3] A. Greenberg, "Hackers remotely kill a Jeep on the highway – with me in it," WIRED, July 21, 2015.

[4] D. Lodge, “Hacking the Mitsubishi Outlander PHEV hybrid,” PenTestPartners, June 05, 2016.
[5] FD. Garcia, D. Oswald, T. Kasper and P. Pavlidès, “Lock It and Still Lose It —on the (In)Security of Automotive Remote Keyless Entry Systems,” in Proc. 25th USENIX Security, Austin, TX, 2016.
[6] R. Hull, “Nissan disables Leaf electric car app after revelation that hackers can switch on the heater to drain the battery,” Thisismoney, Feb. 26, 2016.
[7] R. Link, “Is Your Car Broadcasting Too Much Information?,” Trend Micro Inc., July 28, 2015.
[8] S. Curtis, “Self-driving cars can be hacked using a laser pointer,” The Telegraph, Sept. 08, 2015.
[9] TU-Automotive Ltd, TU-Automotive Cyber Security Europe, 2-3 November 2016, ICM - Internationales Congress Center München, Germany.
[10] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche and Y. Laarouchi, “Survey on security threats and protection mechanisms in embedded automotive networks,” in Proc. IEEE DSN-W, Budapest, June 2013, pp. 1-12.
[11] T. Zhang, H. Antunes and S. Aggarwal, “Defending Connected Vehicles Against Malware: Challenges and a Solution Framework,” IEEE Internet of Things, vol. 1, no. 1, Feb 2014.
[12] D. K. Nilsson and U. E. Larson, “Simulated attacks on can buses: vehicle virus,” in Proc. Int. Conf. on Communication Systems and Networks, Langkawi, Malaysia, 2008, pp. 66-72.
[13] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno,
“Comprehensive experimental analyses of automotive attack surfaces,” in Proc. 20th USENIX Security, San Francisco, CA, 2011.
[14] W. Yan, “A Two-year Survey on Security Challenges in Automotive Threat Landscape,” in Proc. IEEE ICCVE, Shenzhen Oct. 2015, pp. 185-189.
[15] N. Lyamin, A. Vinel, M. Jonsson and J. Loo, “Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks,” IEEE Commu. Letters, vol. 18, no. 1, pp. 110-113, Jan. 2014.
[16] Ericsson, “Connected Vehicle Cloud Under the Hood,” Ericsson, 2015.
[17] National Highway Traffic Safety Administration, “Cybersecurity Best Practices for Modern Vehicles,” Report No. DOT HS 812 333, Washington, DC, Oct 2016.