American Journal of Applied Sciences 11 (2): 337-346, 2014
ISSN: 1546-9239

doi:10.3844/ajassp.2014.337.346 Published Online 11 (2) 2014 (http://www.thescipub.com/ajas.toc)

SECURITY IN VEHICULAR AD HOC NETWORK BASED ON INTRUSION DETECTION SYSTEM

[1]Omkar Pattnaik and [2]Binod Kumar Pattanayak

[1]Department of Computer Science and Engineering,
Synergy Institute of Engineering and Technology, Dhenkanal, ODISHA, Postal Zip-759001, India
[2]Department of Computer Science and Engineering, Institute of Technical Education and Research,
Siksha 'O' Anusandhan University, Bhubanweswar, ODISHA, Postal Zip-751030, India

Received 2013-11-19; Revised 2013-11-28; Accepted 2013-12-27

ABSTRACT

Implementation of mobile ad hoc networks has eventually captured practically most of the parts of day-to-day life. One variation of such networks represents the Vehicular Ad Hoc Networks (VANETs), widely implemented in order to control day-to-day road traffic. The major concern of VANETs is oriented around providing security to moving vehicles that makes it possible to reduce accidents and traffic jam and moreover to establish communication among different vehicles. In this study, we analyze a number of possible attacks that may pertain to VANETs. Intrusion detection imposes various challenges to efficient implementation of VANETs. To overcome it, several intrusion detection measures have been proposed. The Watchdog technique is one of them. We detail this technique so as to make it convenient to implement it in our future investigations.

Keywords: VANET, Attacks, Intrusion Detection and Watchdog

1. INTRODUCTION

In the current technology, the industry and academic research community focus on vehicular networking which has gained a lot of popularity. This concept may be used to provide safety to the transportations systems in an efficient way. Vehicular Ad Hoc Networks (VANET) was created in October 2002 by the Federal Communications Commission (FCC). The aim of its creation was to improve safety on the roads and transportations. The VANET belongs to the customized version of IEEE 802.11, namely IEEE 802.11p. Vehicular ad hoc network is a special form of MANET which is a vehicle to vehicle and vehicle roadside wireless communication network. It is also called as a subclass of MANET. In a typical VANET environment, we assume that each vehicle consists of an On-Board Unit (OBU) and a Road-Side Unit (RSU) installed along the roads. A protocol is used to communicate between OBUs and RSUs, called Dedicated Short Range Communications (DSRC) protocol. But, using a secure fixed network (e.g., the Internet) the RSUs, Trusted Authority (TA) and the application servers communicate with each other. The arbitrary vehicles are allowed to broadcast safety messages (e.g., road condition, traffic accident information) to other nearby vehicles and RSU which is the main objective of VANET (Jamshidi and Karimzadeh, 2011). Intrusion Detection System (IDS) is an effective technique to identify an attack occurring in a VANET. The abnormal or suspicious activities are identified by an Intrusion Detection System (IDS) in a network or host. IDSs are responsible for detecting both internal as well as external attacks. The internal attacks are not detected by cryptographic solutions. Thus, an IDS is often used as one second line of defense after the cryptographic systems.

The rest of the paper is organized as follows. Section 2 represents the characteristics of VANET. Section 3 details the network architecture of VANET. Section 4 discusses the background of IDS. Section 5

Corresponding Author: Omkar Pattnaik, Department of Computer Science and Engineering, Synergy Institute of Engineering and Technology, Dhenkanal, ODISHA, Postal Zip-759001, India

includes Possible Attacks in VANET. Section 6 addresses IDS Techniques for VANET. Section 7 concludes this work.

2. CHARACTERISTICS OF VANET

The unique characteristics of VANET (**Fig. 1**) that are different from MANET, present more challenges and the designing of VANET is more complex.

2.1. Highly Dynamic Topology

When the vehicles are moving at high speed, the topology of VANET changes frequently. Suppose two vehicles are moving at the speed of 30m/sec and the radio range between them is 180 m. Then the link between the two vehicles will last 180/30 = 6 sec (Ibrahim and Bikas, 2011).

2.2. Frequent Disconnected Network

When two moving vehicles exchange their information frequently, they may get disconnected due to its highly dynamic topology. This disconnection will occur mostly in sparse network.

2.3. Mobility Modeling

The traffic environment, roads structure, the speed of vehicles and driver's driving behavior are responsible for the pattern of mobility.

2.4. Battery Power and Storage Capacity

In MANETs, battery power is consumed during the communication, but in VANETs, enough computing power is available since in modern vehicles, battery power and storage is unlimited.

2.5. Communication Environment

In dense networks, the building, trees and other objects may be present that behave as obstacles in the network, but in sparse network like high-way, these things are absent. Thus, the routing approach of sparse and dense networks must be different (Reichardt *et al*., 2002).

3. NETWORK ARCHITECTURES

Wireless ad hoc networks generally do not depend on fixed infrastructure for communication and dissemination of information. VANETs follow the same principle because it is a subclass of MANET. It can be applied to surface transportation with highly dynamic environment. As shown in **Fig. 2**, the architecture of VANETs can mainly be classified into three categories: Pure cellular/WLAN, pure ad hoc and hybrid (Kumar and Dave, 2011). **Figure 2(a)** represents pure cellular environment where VANET can be worked out. Similarly all vehicles and road-side wireless devices can form a pure mobile ad hoc network (**Fig. 2(b)**) to perform Vehicle to Vehicle (V2V) communications and achieve certain goals.

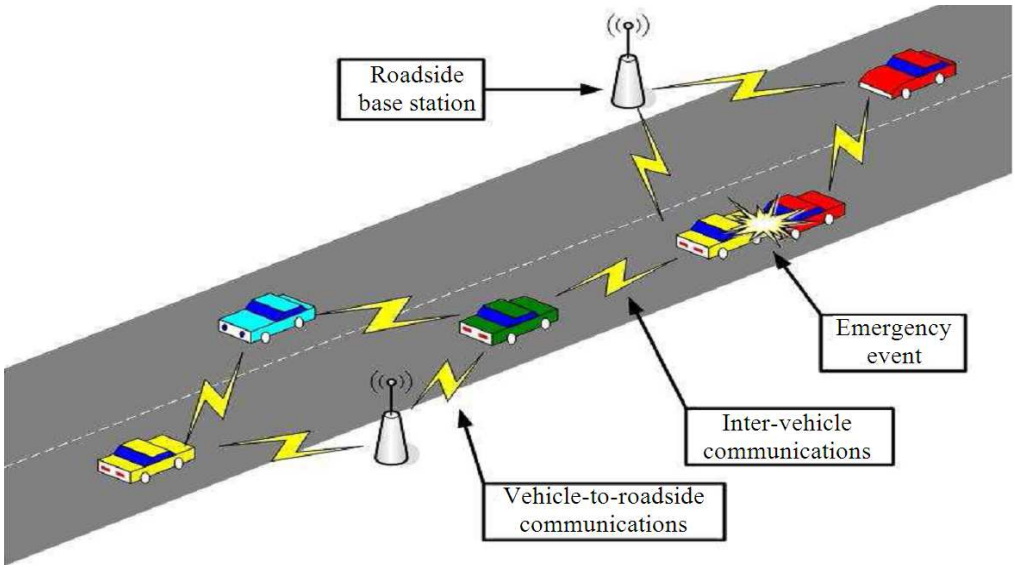

Fig. 1. A VANET consisting of vehicles and road-side base stations that exchange primarily safety messages to give the drivers time to react to life-endangering events (Ibrahim and Bikas, 2011)

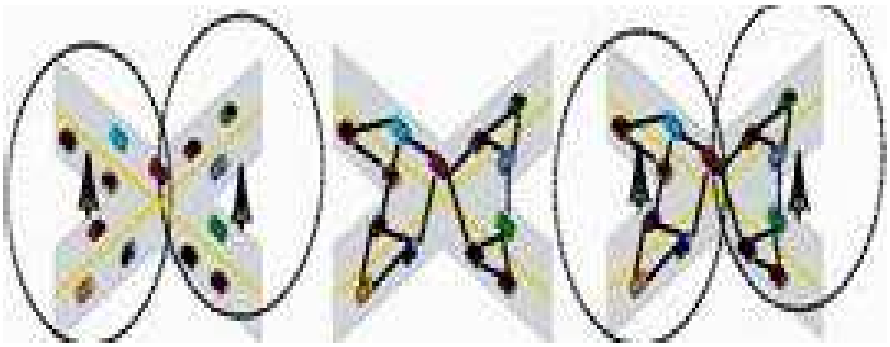

Fig. 2. Network architectures for VANETs (a) Cellular/WLAN (b) Ad Hoc (c) Hybrid

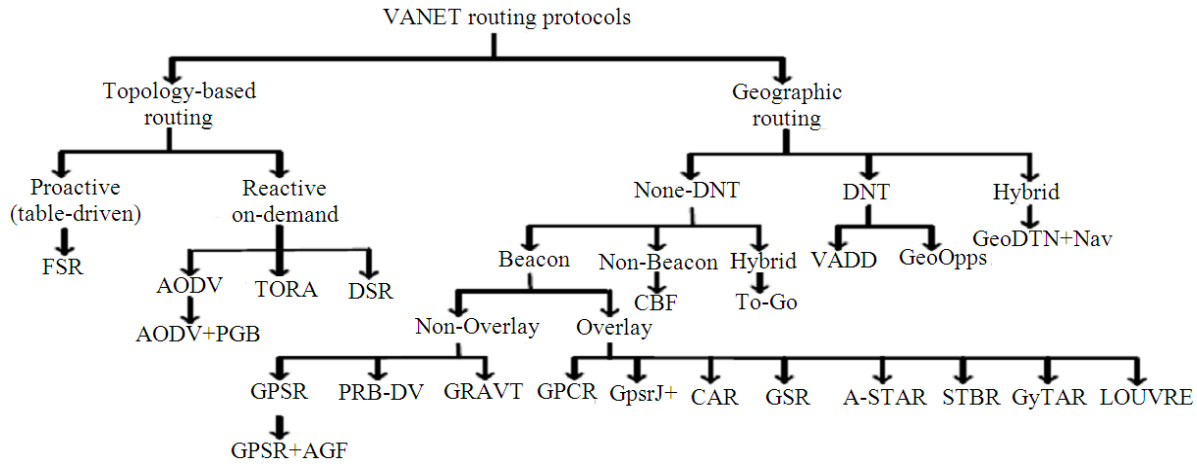

Fig. 3. Taxonomy of various routing protocols (Abolhasan *et al*., 2004)

Figure 2c depicts the hybrid architecture meaning combination of cellular network and ad hoc network. A better coverage can be provided by the hybrid architecture, but it creates new problems, such as the seamless transition of the communication among different wireless systems.

3.1. Taxonomy of Various Routing Protocols in VANET

The routing protocols in VANET can be classified as two groups: (i) topology-based routing and (ii) geographic routing. To perform packet forwarding in the network, the information about links that exist in the networks are used. But in geographic routing, neighboring location information are used to perform packet forwarding. The different types of routing protocols in VANET are shown in **Fig. 3** (Bernsen and Mnivannan, 2009).

4. BACKGROUND OF INTRUSION DETECTION SYSTEM (IDS)

An Intrusion-Detection System (IDS) can be defined as the tools, methods and resources to help identify, assess and report unauthorized or unapproved network activities. Intrusion detection is typically a part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure (Ngadi *et al*., 2008). The purpose of intrusion detection is to serve as an alarm mechanism for a computer system or a network. It provides information of unwanted or misbehaving elements and isolates those elements to deny them from accessing the computer or network resources. It is possible to identify three main modules in an IDS (**Fig. 4**): A Monitoring Module, controlling the collection of data; an Analysis Module, deciding if the data collected indicate an intrusion or not;

and a Response Module, managing the response actions to the intrusion (**Fig. 1**). Some assumptions are made in order for intrusion detection systems to work (Zhang *et al*., 2003). The First assumption is that user and program activities are observable. The second assumption, which is more important, reveals that normal and intrusive activities must have distinct behavior, as intrusion detection must capture and analyze system activity to determine if the system is under attack. Depending on the detection techniques used, IDS can be classified into three main categories (Hijazi and Nasser, 2005): (1) signature or misuse based IDS; (2) anomaly based IDS; (3) specification based IDS, which is a hybrid of both the signature and the anomaly based IDS. The signature based IDS uses pre-known attack scenarios (or signatures) and compare them with incoming packets traffic. There are several approaches in the signature detection, which they differ in representation and matching algorithm employed to detect the intrusion patterns. The detection approaches, such as expert system (Lunt *et al*., 1988), pattern recognition (Esposito *et al*., 2005), colored petrinets (Kumar and Spafford, 1994) and state transition analysis (Porras and Kemmerer, 1992) are grouped as misuse categories.

Meanwhile, the anomaly-based IDS attempts to detect activities that differ from the normal expected system behavior. This detection has several techniques, i.e.: statistics (Porras and Valdes, 1998), neural networks (Forrest *et al*., 1997) and other techniques such as immunology (Lee *et al*., 1999), data mining (Ye *et al*., 2001) and Chi-square test utilization (Debar *et al*., 2000). Moreover, a good taxonomy of wired IDSs was presented by (Ko *et al*., 2001).

The specification-based IDS monitors current behavior of systems according to specifications that describe desired functionality for security-critical entities (Zhang and Lee, 2000). A mismatch between current behavior and the specifications will be reported as an attack. Anomaly detection (**Fig. 5**) bases its idea on statistical behavior modeling and anomaly detectors looking for behavior that deviates from normal system use. A typical anomaly detection system takes in audit data for analysis. The audit data are transformed to a format statistically comparable to the profile of a user. The user's profile is generated dynamically by the system (usually using a baseline rule laid by the system administrator) initially and subsequently updated based on the user's usage. Thresholds are normally always associated to all the profiles (Pattnaik and Pattanayak, 2012). If any comparison between the audit data and the user's profile resulted in deviation, crossing a threshold set, an alarm of intrusion is declared.

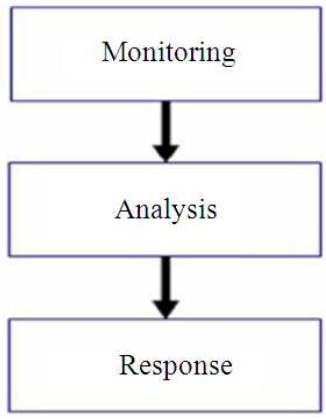

Fig. 4. IDS basic modules

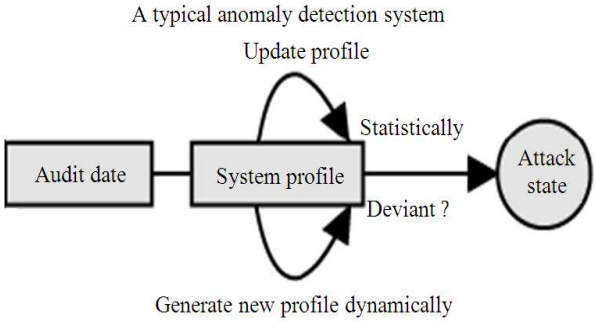

Fig. 5. Example of anomaly detection system

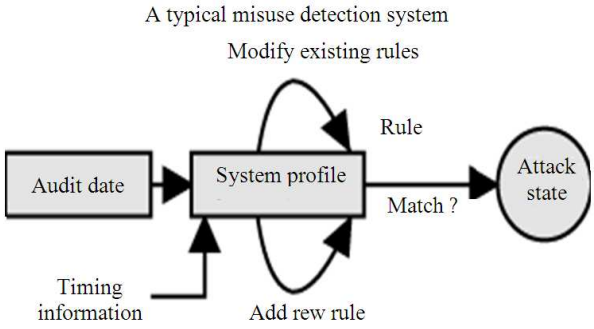

Fig. 6. Example of a misuse detection system

This type of detection systems is well suited to detect unknown or previously not encountered attacks.

The second type of model bases its detection upon a comparison of parameters of the user's session and the user's commands to a rule base of techniques used by attackers to penetrate a system. Known attack methods are what this model looks for in a user's behavior. Since

this model looks for patterns known to cause security problems, it is called a "misuse" detection model (**Fig. 6**). It is obvious that the enemies, knowing that intrusion prevention and detection systems are in our networks, will attempt to develop and launch new types of attacks. In anticipation of these trends, IDS researchers are designing techniques for combining anomaly and misuse detection and system architecture for distributed and coordinated intrusions.

5. POSSIBLE ATTACKS IN VANET

There are 3 types of attacks possible in VANET. They are: Threat to driver confidentiality, threat to availability and threat to authenticity.

5.1. Threats to Confidentiality

The location information available through the transmission of broadcast messages and the gathering of illegitimate collection of messages through eavesdropping are responsible when confidentiality of messages exchanged between the nodes of a vehicular network are more vulnerable. The attackers may be insiders or outsiders and can collect the information about road users without their knowledge and use the information at a time when the user is unaware of the collection. The vehicle users have important issues such as Location privacy and anonymity (Rawat *et al*., 2012).

5.2. Traffic Analysis

In this type of attack, the privacy of user in VANET is compromised. The attacker tries to analyze the traffic packet on the Vehicle-to-Vehicle (V2V) or Vehicle-to-Road Side Unit (V2RSU) (Lunt *et al*., 1988). To extract the required information of a user, the attacker uses the packet which contains location of Vehicle ID and traveling path of the vehicle (Zeadally *et al*., 2012).

5.3. Social attack (Fig. 7)

In social attack, the attacker creates confusion and bedazzles the victim by sending unethical and unmoral message to the drivers so that the driver gets disturbed and reacts in annoyed manner that affects its driving and that strongly affects in the network. This is the main objective of the attacker (Sumra *et al*., 2011a).

5.4. Brute Force

In VANET, many applications of cryptographic algorithms and approaches are implemented to protect against the threat. The attacker can use brute force technique to break the cryptography key (Isaac *et al*., 2010).

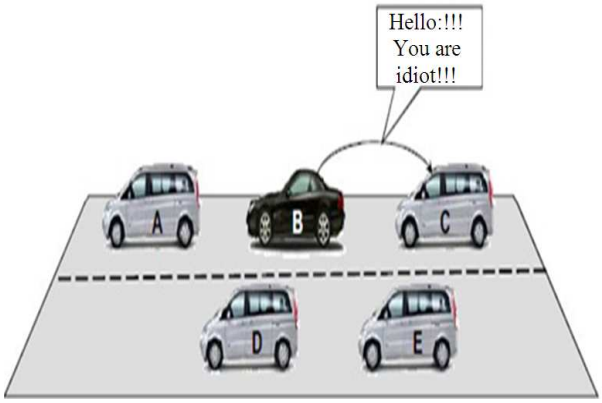

Fig. 7. Social attack

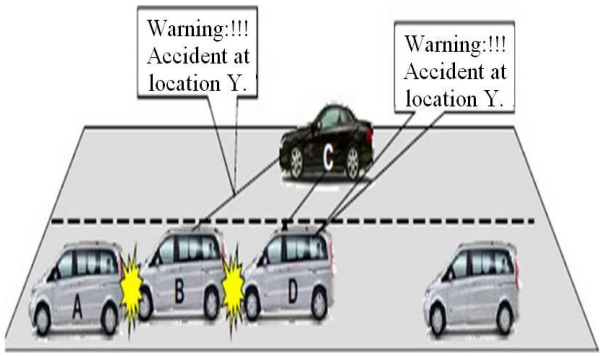

Fig. 8. Timing attack

5.5. Timing Attack (Fig. 8)

Time is an important issue in Intelligent Transportation System (ITS) safety applications. So users need accurate information at right time without any delay. In this attack, the attacker does not manipulate the actual content rather it adds some time slot to create a delay in the message. So the user will receive the message after the required time (Sumra *et al*., 2011a). ITS safety applications are time critical applications which require data transmission in time, failing which major accidents can happen.

5.6. Threats to Availability

Denial of Service (DOS) attack (**Fig. 9**): The main objective of DOS attack is to prevent the user from accessing the network services and resources. The user cannot communicate in the network and pass information to other vehicle which could result in more devastation in life critical application (Soomro *et al*., 2010). This is most serious problem in VANET. There are three different ways as attacker can achieve it:

- In basic level, the attacker overwhelm the node resource so that it cannot perform other necessary tasks which results in becoming the node continuously busy and not able to do anything else
- In extended level, the attacker jams the channel by generating high frequency in the channel so that no vehicle is able to communicate to other vehicle in the network
- Drop the packets

Black Hole Attack: When a node refuses to participate in the network or when an established node drops out, it's called as black hole attack. In this attack, the entire traffic of the network gets redirected towards a specific node. But, that node does not exist actually which results in loss of data. The malicious node chooses whether to drop a packet to perform a denial-of-service attack.

Spamming: The attacker sends spam messages in the network to consume the bandwidth of network and to increase the transmission latency. Due to lack of necessary infrastructure and centralized administration, it becomes difficult to control (Sumra *et al*., 2011b). These messages are of no concern to the user and are just like advertisement messages.

5.7. Threats to Authentication

5.7.1. Sybil attack (Fig. 10)

In Sybil attack, multiple messages are transmitted by the attacker from different IDs to the other vehicles and create illusion that messages are coming from different vehicles. So there is a jam further and they are enforced to take alternate route (Douceur, 2002). It is a critical attack. The main task of the attacker is to provide an illusion of multiple vehicles to other vehicles and to enforce them to choose alternate routes.

5.8. Node Impersonation Attack (Fig. 11)

In VANET, each vehicle is identified by its unique ID and with the help of this ID; it can be located in the network easily when an accident happens. An attacker can change his/her identity and acts like a real originator of the message in impersonation attack. An attacker receives the message from the originator of the message and changes the contents of the message for his/her benefits. Then it sends it to other vehicles.

Replay: When attacker replays the transmission of previously generated frames in new connections, then replay attack takes place.

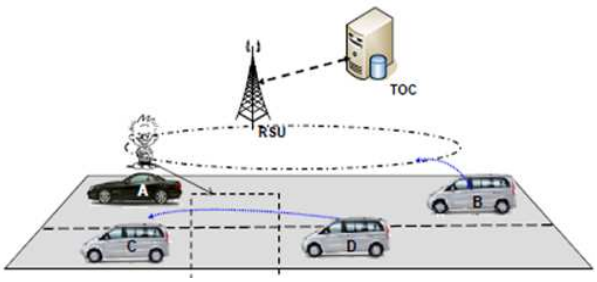

Fig. 9. DOS attack

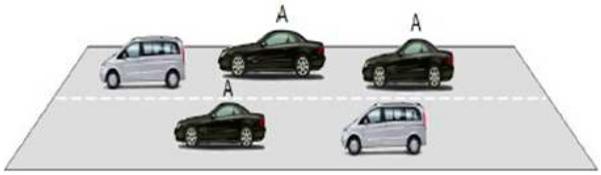

Fig. 10. Sybil attack

It is basically used by authorized or malicious user to masquerade as a legitimate user or Road Side Unit (RSU). The attacker captures a generated frame and uses it in other parts of the networks (Samara *et al*., 2010). It does not contain timestamp or sequence number and so, we don't have any protection against this attack currently. The main objective of this attack is to mystify the authorities and prevent identification of vehicle in any accident.

Tunneling: In this type of attack, two distant parts of the Ad hoc network is connected by attacker using an extra communication channel as a tunnel. In this case, the nodes are assumed that they are neighbors and send data using the tunnel (Saini and Kumar, 2010). The attacker has the possibility of conducting a traffic analysis or selective forwarding attack.

6. IDS TECHNIQUES FOR VANET

To establish communication routes using routing protocols, nodes exchange network topology information. VANET devices (also called nodes) act both as computers and routers. In routing protocols, mainly two types of threats are possible. The first comes from external attackers and the second one is more severe kind of threat coming from compromised nodes. In case of first one, a network may be partitioned and traffic overload occurs due to retransmission and inefficient routing, since the attacker can perform injecting erroneous routing information, replaying old routing information, or distorting routing information.

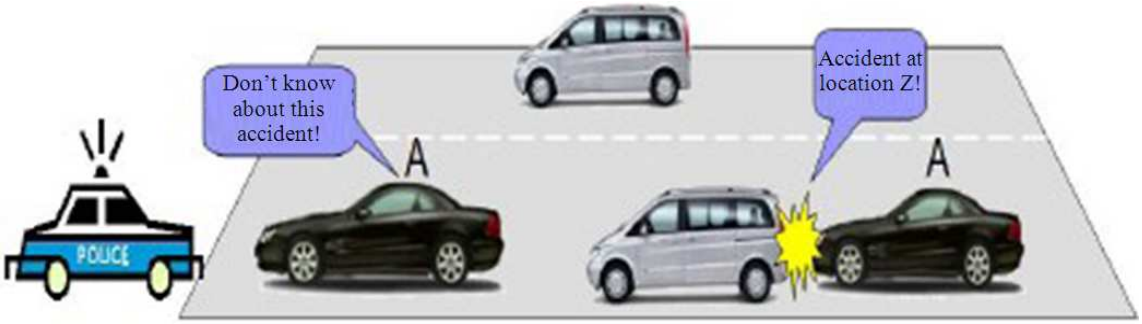

Fig. 11. Node Impersonation attack

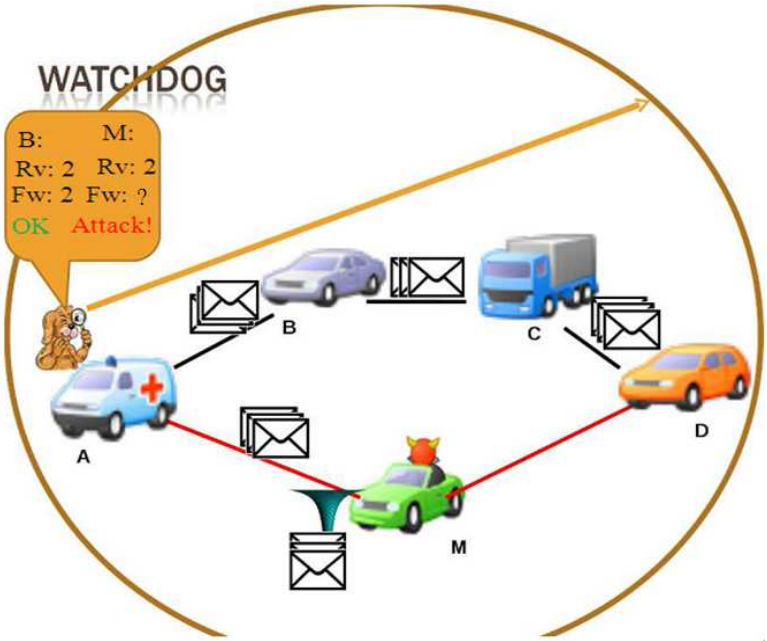

Fig. 12. The watchdog technique

In second case, the node might be (i) misusing routing information for other nodes or (ii) acting on applicative data in order to induce service failures (Hu and Perrig, 2004). In earlier studies, it was mentioned that the watchdog is the basic mechanism in an intrusion detection system (Brutch and Ko, 2003; Obimbo *et al*., 2006). The activity can be monitored by a node which can listen to the packets traversing its neighborhood information. This is the main idea behind this type of IDS. So the watchdogs act in promiscuous mode, thus overhearing all next nodes forwarding transmissions. When the nodes are acting as selfish or black hole routers, the watchdog can deduce information of neighborhood behavior. This technique is independent of the technology and routing protocols used in these kinds of attacks. **Figure 12** shows a basic example of the watchdog behavior. Vehicle "A" can send packets to vehicle "D" either using the route "{A-B-C-D}" or "{A-M-D}". The watchdog can listen to the packets forwarded by B and M who are in range. "B" forwards all packets to "C" but "M" performs a black hole attack and drops all received packets. When "M" does not send the packet, the watchdog knows it and marks it as an attacker. The watchdog is used as the basic brick of a IDS solutions. The information provided by watchdogs are used to rate neighbors. This is the mechanism of Pathrater (Marti *et al*., 2000).

In Route guard mechanism (Hasswa *et al*., 2005), the watchdog and pathrater are combined to provide a solution to classify each neighbor node as Fresh, Member, Unstable, Suspect or Malicious. In ad hoc networks, watchdogs represent the core of most important types of IDS solutions. So the design and implementation of such components is complex and it is critical to find their detail intrusion detection capabilities. The mobility of nodes and collisions, limits the detection accuracy of watchdogs. So it may produce the false positive conditions. The basic job of watchdog is to count all packets received from its neighbors when a node performs malicious behavior and the packets that must be forwarded (those that are not addressed to the node where the watchdog is under execution). The ratio between the received packets for forwarding and those effectively forwarded by the neighbor node is called neighbor trust level. So it is assumed that the node, forwarding all received packets, has a neighbor trust level of 1, meaning 100%. When the received packets are not forwarded by the node, the watchdog changes its state to untrusted and marks it as malicious node. We assume that an ideal neighbor trust level is 1 (100%) always but in practice, such value level is rarely attained. Authors in (Murugan and Shanmugam, 2010) address a combined solution for routing and MAC layer attacks for mobile ad hoc networks. Authors in their approach, incorporate three different techniques simultaneously to achieve their goal: (i) a cumulative frequency detection technique in order to detect MAC layer attacks; (ii) data forwarding behavior based technique in order to detect dropped packets and (iii) message authentication code based technique for modification of packets.

7. CONCLUSION

The intrusion detection in VANETs is a challenging task due to its frequently changing network topology and deployed applications. Every individual wants to stay safer and secured on the road during driving. In this study, we focus on some characteristics of VANETs with possible types of attacks based on intrusion detection. Also we discuss the most suitable IDS technique like watchdog with their effect in VANETs. The application of VANETs is a rising technology which can provide the future directions of research in vehicular environment. In future, we intend to study the detection technique of watchdog thoroughly and implement using ns-2 simulator. Doing so, we need to try to minimize the rate of false positive condition by improving the trust level practically.

8. REFERENCES

Abolhasan, M., T. Wysocki and E. Dutkiewicz, 2004. A review of routing protocols for mobile ad hoc networks. Ad Hoc Netw., 2: 1-22. DOI: 10.1016/S1570-8705(03)00043-X

Bernsen, J. and D. Mnivannan, 2009. Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification. J. Pervasive Mobile Comput., 5: 1-18. DOI: 10.1016/j.pmcj.2008.09.001

Brutch, P. and C. Ko, 2003. Challenges in intrusion detection for wireless ad-hoc networks. Proceedings of the Symposium Applications and the Internet Workshops, Jan. 27-31, IEEE Xplore Press, pp: 368-373. DOI: 10.1109/SAINTW.2003.1210188

Debar, H., M. Dacier and A. Wespi, 2000. A revised taxonomy for intrusion-detection systems. Annales Telecommun., 55: 361-378. DOI: 10.1007/BF02994844

Douceur, J., 2002. The Sybil attack. Proceedings of the 1st International Workshop on Peer to Peer (P2P) System, Mar. 7-8, Springer Berlin Heidelberg, MA, USA., pp: 251-260. DOI: 10.1007/3-540-45748-8_24

Esposito, M., C. Mazzariello, F. Oliviero, S.P. Romano and C. Sansone, 2005. Evaluating pattern recognition techniques in intrusion detection systems. Proceedings of the 7th International Workshop on Pattern Recognition in Information Systems, (PRIS' 05), pp: 144-153.

Forrest, S., S.A. Hofmeyr and A. Somayaji, 1997. Computer immunology. Commun. ACM, 40: 88-96. DOI: 10.1145/262793.262811

Hasswa, A., M. Zulkernine and H. Hassanein, 2005. Routeguard: An intrusion detection and response system for mobile ad hoc networks. Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Aug. 22-24, IEEE Xplore Press, pp: 336-343. DOI: 10.1109/WIMOB.2005.1512922

Hijazi, A. and N. Nasser, 2005. Using mobile agents for intrusion detection in wireless ad hoc networks. Proceedings of the 2nd IFIP International Conference on Wireless and Optical Communications Networks, Mar. 6-8, IEEE Xplore Press, pp: 362-366. DOI: 10.1109/WOCN.2005.1436049

Hu, Y.C. and A. Perrig, 2004. A survey of secure wireless ad hoc routing. IEEE Security Privacy, 2: 28-39. DOI: 10.1109/MSP.2004.1

Ibrahim, B.P. and A.N. Bikas, 2011. VANET routing protocols: Pros and cons. Int. J. Comput. Applic.

Isaac, J.T., S. Zeadally and J.S. Camara, 2010. Security attacks and solutions for vehicular ad hoc networks. IET Commun., 4: 894-903. DOI: 10.1049/iet-com.2009.0191

Jamshidi, K. and M. Karimzadeh, 2011. Providing security in Vehicular Ad hoc Networks (VANETs) through historical data collection. Int. J. Comput. Sci. Eng., 3: 1393-1398.

Ko, C., P. Brutch, J. Rowe, G. Tsafnat and K. Levitt, 2001. System health and intrusion monitoring using a hierarchy of constraints. Proceedings of 4th International Symposium, Oct. 10-12, Springer Berlin Heidelberg, Davis, CA, USA., pp: 190-203. DOI: 10.1007/3-540-45474-8_12

Kumar, R. and M. Dave, 2011. A comparative study of various routing protocols in VANET. Int. J. Comput. Sci. Issu.

Kumar, S. and E.H. Spafford, 1994. A pattern matching model for misuse intrusion detection. Proceedings of the 17th National Computer Security Conference, (NCSC' 94), pp: 11-21.

Lee, W., S.J. Stolfo and K.W. Mok, 1999. A data mining framework for building intrusion detection models. Proceedings of the IEEE Symposium on Security and Privacy, May 9-12, IEEE Xplore Press, Oakland, California, pp: 120-132. DOI: 10.1109/SECPRI.1999.766909

Lunt, T.F., R. Jagannathan, C. Jalali and P.G. Neumann, 1988. IDES: The enhanced prototype C a real time intrusion detection expert system. Technical Report SRI-CSL-88-12, SRI International, Menlo Park, CA.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Aug. 6-11, ACM Press, Boston, MA, USA., pp: 255-265. DOI: 10.1145/345910.345955

Murugan, R. and A. Shanmugam, 2010. A combined solution for routing and medium access control layer attacks in mobile ad hoc networks. J. Comput. Sci., 6: 1416-1423. DOI: 10.3844/jcssp.2010.1416.142

Ngadi, M.A. and A.H. Abdullah and S. Mandala, 2008. A survey on MANET intrusion detection. Int. J. Comput. Sci. Security, 2: 1-11.

Obimbo, C., L.M. Arboleda and Y. Chen, 2006. A watchdog enhancement to IDS in MANET. Proceedings of the IASTED Conference on Wireless Networks, (CWN' 06).

Pattnaik, O. and B.K. Pattanayak, 2012. Survey on application of IDS in MANET. J. Eng. Applied Sci., 7: 1576-1580.

Porras, P.A. and A. Valdes, 1998. Live traffic analysis of TCP/IP gateways. Proceedings of the ISOC Symposium on Network and Distributed System Security, (NDSS' 92), San Diego, CA.

Porras, P.A. and R.A. Kemmerer, 1992. Penetration state transition analysis: A rule-based intrusion detection approach. Proceedings of the 8th Annual Computer Security Application Conference, Nov. 30-Dec. 04, IEEE Xplore Press, San Antonio, TX, pp: 220-229. DOI: 10.1109/CSAC.1992.228217

Rawat, A., S. Sharma and R. Sushil, 2012. VANET: Security attacks and its possible solutions. J. Inform. Operat. Manage., 3: 301-304.

Reichardt, D., M. Miglietta, L. Moretti, P. Morsink and W. Schulz, 2002. CarTALK 2000: Safe and comfortable driving based upon inter-vehicle-communication. Proceedings of the IEEE Intelligent Vehicle Symposium, Jun. 17-21, IEEE Xplore Press, pp: 545-550. DOI: 10.1109/IVS.2002.1188007

Saini, A. and H. Kumar, 2010. Comparison between various black hole detection techniques in MANET. Proceedings of the National Conference on Computational Instrumentation, Mar. 19-20, CSIO Chandigarh, India, pp: 157-161.

Samara, G., W.A.H. Al-Salihy and R. Sures, 2010. Security issues and challenges of Vehicular Ad Hoc Networks (VANET). Proceedings of the 4th International Conference on New Trends in Information Science and Service Science (NISS), May 11-13, IEEE Xplore Press, Gyeongju, pp: 393-398.

Soomro, I.A., H.B. Hasbullah and J.L. bin Ab Manan, 2010. User requirements model for vehicular ad hoc network applications. Proceedings of the International Symposium in Information Technology, Jun. 15-17, IEEE Xplore Press, Kuala Lumpur, pp: 800-804. DOI: 10.1109/ITSIM.2010.5561602

Sumra, I.A., H. Hasbullah, I. Ahmad, J.L. bin Ab Manan, 2011a. Forming vehicular web of trust in VANET. Proceedings of the Saudi International Electronics, Communications and Photonics Conference (SIECPC), Apr. 24-26, IEEE Xplore Press, Riyadh, pp: 1-6. DOI: 10.1109/SIECPC.2011.5876941

Sumra, I.A., I. Ahmad, H. Hasbullah and J.L. bin Ab Manan, 2011b. Classes of attacks in VANET. Proceedings of the Saudi International Electronics, Communications and Photonics Conference (SIECPC), Apr. 24-26, IEEE Xplore Press, Riyadh, pp: 1-5. DOI: 10.1109/SIECPC.2011.5876939

Ye, N., X. Li, Q. Chen, S.M. Emran and M. Xu, 2001. Probabilistic techniques for intrusion detection based on computer audit data. IEEE Trans. Syst. Man Cybernetics, 31: 266-274. DOI: 10.1109/3468.935043

Zeadally, S., R. Hunt, Y.S. Chen, A. Irwin and A. Hassan, 2012. Vehicular Ad hoc Networks (VANETS): Status, results and challenges. Telecommun. Syst., 50: 217-241. DOI: 10.1007/s11235-010-9400-5

Zhang, Y. and W. Lee, 2000. Intrusion detection in wireless ad-hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Aug. 6-11, ACM Press, Boston, MA, USA., pp: 275-283. 10.1145/345910.345958

Zhang, Y., W. Lee and Y.A. Huang, 2003. Intrusion detection techniques for mobile wireless networks. Wireless Netw., 9: 545-556. DOI: 10.1023/A:1024600519144