International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 1 Issue 6 December 2015

Optimized Authentication Mechanism for Vehicular Ad Hoc Networks

Ranjana Verma[1], Shivani Shrivastri[2]

M-tech scholar RGPM, Bhopal[1], Asst. Prof. Dept. of CSE, RGPM Bhopal[2]
ranuverma02@gmail.com[1], shivani.shrivastri@gmail.com[2]

ABSTRACT:- Vehicular ad-hoc networks (VANETs) have started to receive increasing interest recently due to their potential to be used in trace and safety applications in the upcoming years. Recently authentication schemes were to lower communication overhead, preserve node anonymity, isolation of misbehaving nodes, and non-repudiation. Research directions are aimed at implementing a Trust Validation Model to reduce the vulnerability window on infrastructure-less scenarios, which includes exploring reputation based systems, and more efficient revocation information distribution mechanisms.

KEYWORDS:- VANET, DoS Attack, Authentication code, Ant colony optimization.

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) have started to receive increasing interest recently due to their potential to be used in traffic and safety applications in the upcoming years [6] [7]. In such an ad hoc network, vehicles equipped with a wireless transmission device can send and receive messages at significantly higher speeds compared to traditional mobile ad-hoc networks [8]. Vehicles exchange traffic information as they move through the network, which allows drivers to adjust their routes to avoid congestion, obtain road-condition warnings, and be warned in advance for potential traffic accidents.

While the majority of recent research focused on medium access control and routing protocols with the goal of handling the dynamic behavior of VANETs [7] [9], an important aspect that needs to be considered is the security in transmitting messages. Security of VANETs is critical in preventing collisions and thus minimizing the risk for major accidents. For instance, all safety-related messages sent by a vehicle must be verified by the recipient for its authenticity and integrity in face of adversaries that may inject messages containing bogus information to the network. Yet the privacy of the driver sending those safety-related messages against unauthorized observers must be guaranteed. However, this anonymity service should be made conditional, meaning it can be revoked for law enforcement purposes whenever necessary. Besides those aforementioned requirements, a secure VANET system should also support availability against various common attacks such as denial-of-service (DoS) attacks and replay attacks.

II. Vehicular Ad-Hoc Networks (VANETs)

In the last few years, accompanying the massive deployment of wireless technologies and the growing number of wireless products on motorized vehicles including remote keyless entry devices, personal digital assistants (PDAs), laptops, and mobile telephones, automotive industries have opened a wide variety of possibilities for both drivers and their passengers. Vehicular Ad hoc Networks (VANETs) have attracted a lot of attention in research community because of their varied value added services, namely vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based service for finding the closest fuel station, travel lodge or restaurant and simply access to the Internet [1], [5].

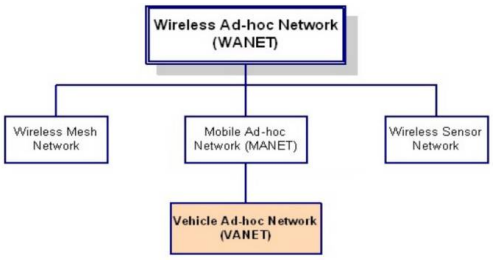

Figure 1:- Hierarchy of Wireless Ad Hoc Networks

However, many forms of attacks against VANETs have emerged recently and alarmed the unsettling situation of these networks' security. Being an implementation of Mobile Ad hoc Networks (MANETs) (Fig.1), VANETs inherit all the discovered and undiscovered security and privacy vulnerabilities related to MANETs. Furthermore, VANETs have a number of distinctive properties [5] that could be also vulnerabilities for attackers to exploit. Those properties include the particular nature of communication in VANETs. Connections in a VANET in particular and in any Wireless Ad hoc Network in general are based on node-to-node

communications: every node is able to act as either a host inquiring data or a router forwarding data. There are two types of nodes: (i) Road Side Units (RSUs) standing for fixed nodes provisioned along the route and (ii) On Board Unit (OBU) referring to mobile nodes (i.e., vehicles) equipped with some sort of radio interface that enables connecting to other nodes in wireless manner. Fig. 2 depicts a general view of VANETs structure. It is worth mentioning that the speed of mobile nodes- vehicles in VANETs may be much higher than in MANETs. This reason makes VANETs very dynamic in nature. A number of nodes can communicate once as a group but can then rapidly change their own structure caused by leaving of a member or joining of another node. Therefore, it is expected that nodes are continuously "keeping in touch" with other nodes in the group to maintain the survival of the network. This aspect of VANETs seems to be very vulnerable and attacks can be unconsciously or intentionally performed to damage a part of or the total network. As mentioned above, VANETs provide many added applications that are safety, entertainment, or infotainment oriented. Attacks to VANETs may lead to catastrophic consequences such as the losses of lives in the case of traffic accident, losses of time (e.g., tampering traffic jam made by attacks) or financial losses (i.e., in payment services).

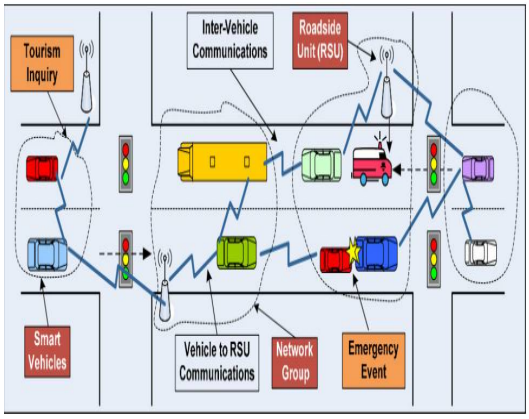

Figure 2:- Basic Structure of Vanets [5]

Vehicular ad-hoc networks (VANETs) have started to receive increasing interest recently due to their potential to be used in trace and safety applications in the upcoming years [2] [3]. In such an ad hoc network, vehicles equipped with a wireless transmission device can send and receive messages at significantly higher speeds compared to traditional mobile ad-hoc networks [4]. Vehicles exchange trace information as they move through the network, which allows drivers to adjust their routes to avoid congestion, obtain road-condition warnings, and be warned in advance for potential trace accidents.

III. LITERATURE SURVEY

The most common objectives of recent authentication schemes were to lower communication overhead, preserve node anonymity, isolation of misbehaving nodes, and non-repudiation. These, however, were not the only objectives stated in the following works. One keynote is that most of the works aimed at providing various security properties which would be appropriate for one particular application or privacy level, but is more than required for another.
In year 2012, author Ajay Kushwaha &Hariram Sharma [7] introduced an enhanced approach of selective encryption algorithm for better security of data. This method ensures that the infrequent words or sensitive data can encrypted. They carried NS-2 simulator for simulation of proposed method. Their method ensures that the infrequent or sensitive data will be encrypted and this algorithm also eliminates the unwanted data like parts of speech (prepositions, articles, conjunctions, models, etc., so they will provide more security. Text data contains parts of speech, such as articles, reposition, conjunction, modals and interjection encryption of all these parts consists large overhead in encryption but their approach can removes all these overhead of data. Their method use encryption only on sensitive data and encrypt them and send it to the destination. By this, overhead of data is reduced & improved security of data.

In 2012, author Adarsh, Krishna and Alok Aggarwal, et al. [11], proposed a novel integration mechanisms to provide complete cryptography services for MANETs. They shows that DSDV performance better than AODV and DSR when discovery approach will change into reactive approach. They showed an effective way to gain authentication, privacy, key management, availability and non-repudiation. For security of MANETs low GEs are required and it gives maximum delay and throughput. Therefore, it can be implemented with stream ciphers with less number of GEs. It requires low rate equivalents and give maximum throughput so that it proved that this approach satisfy all need of secure MANET.

In year 2012, author Ahmad Ali, Lin Cai and Fayez Gebali, et al, [3], proposed a new MAC protocol called "Dual-sensing directional MAC (DSDMAC)" protocol with directional antennas for wireless ad-hoc networks. This DSDMAC protocol provides dual-sensing scheme to identify hidden-terminal problem and to resolve it.DSDMAC protocol depends on dual sensing method that can identify the deafness, it can avoid unnecessary blocking and it can solve the hidden terminal problem. Integrity of DSDMAC can verified and validated using Spin. Spin is a verification and validation tool which verify the correctness of analysis. The analysis and verification of protocol and robust simulation of DSDMAC can ensure the

higher network throughput and lower delay with the directional antennas. According to this paper, DSDMAC performs better than other existing protocols based on Spins result. It proved that enhancing performance of wireless network using directional antennas.

In year 2013, author Peng Zhang Lin, Yixin Jiang, Yanfei Fan &Xuemin Shen, et al.[2], proposed a method for secure property for network coding. They describe a new technique i.e. P-coding, it is a lightweight encryption scheme to protect the data from external eavesdropper in network coded MANETs. The main idea is to divide data into generations and generate PEF key. Then global encoding vector will chooses randomly and appended to the message. There is a Key Distribution Center which can create PEF keys and distribute in each generation between sender and receiver. PEF key can disclose in any generation due to various number of generation but key is generated in each generation separately so that this method can protect security from single generation failure. In this, P-coding used permutation encryption by which data symbols can randomly mixes with its coding vector, it makes hard for eavesdropper to decode the data. So that, this paper proved that security can enhanced by permutation encryption technique.

In 2013, author Yao, Lin, Deng, Miao and Yim&Guowei Wu, et al. [10], proposed anonymous mutual authentication based on biometrics in VANETs. According to this paper, during authentication phase, two vehicles negotiate their temporary session key and produce two temporary MAC address. Authentication procedure matched the user's biometric and stored templates in database by using field sampling. This will shows the user identity. This method generates two temporary MAC address for security against eavesdropper. For communication a unique key is also created for encryption. Their privacy analysis proves that K-anonymity is gained to secure the identity of each user.

In year 2013, author Prakashgoud Patil and Umakant Kulkarni, et al. [1], proposed a method called "Support Vector Machine based Data Redundancy Elimination for Data Aggregation in WSN (SDRE)". This SDRE can reduce the redundant data and eliminate false data from wireless sensor network. In this paper, they built an aggregation tree of sensor network size and SVM method applied on data to remove redundancy. They used Local Sensitive Hashing for minimize redundant data and false data. LSH works based on data similarity and their threshold. This LSH code are send to aggregator supervisor node of tree, this sensor node will find same data node and select only one node for sending data. Aggregator supervisor can also reduce outliers and it does not receive data from another node. It proved improve performance of WSN based on such parameters as delay, energy, packet drops and overheads.

In year 2013, author Emiliano and Claudio Soriente, et al. [5], proposed a scheme in which, they focus on security in Participatory Sensing and provide a suitable secure infrastructure. They define Privacy-Enhanced Participatory Sensing Infrastructure. This paper provides a set of rules of privacy need for both data sender and receiver. Then, they defines an effective solution for mobile phone users with very low overhead. They proved that the Participatory Sensing application enhance privacy and user participation. Firstly they definea set of definitions for privacy needs for both the data sender and data receiver. Then for mobile phone users, they proposed an efficient and easy solution. They also proposed an efficient cryptographic approach that includes privacy. Participatory Sensing have great potential and it is novel computing technique. Their solution is adaptable by recent Sensing Applications that provides security and increase user participation with low overhead.

IV. VANET CHALLENGES

A VANET environment has to overcome assured issues of limitation and inefficiency. It includes [5]:

A. The Wireless Link Characteristics are Time-varying in Nature – There are transmission disorders like path loss, fading, obstacle and interference that introduce susceptible nature of wireless medium. The reliability of wireless communication is struggled by different issues.

B. Limited Range of Wireless Transmission – The limited radio range outcomes in reduced data rates to the wireless networks. Therefore ideal consumption of bandwidth is required by keeping limited overhead as possible.

C. Packet Losses Due to Errors in Transmission – VANETs high packet loss collisions, interference, wireless channel issues, and often influenced by the effects of path-breaking devices, unidirectional links due to the existence of hidden terminals on the other hand, due to the increased mobility of collisions.

D. Route Changes Due to Mobility – The dynamic network topology results in frequent path breaks.

E. Frequent Network Partitions –The arbitrary movement of devices leads partition of network. This frequently affects the intermediate devices.

F. Energy Efficiency – Today mostly devices are operated by batteries so it is a major issue to save power or energy for frequent data packet forwarding from source to destination.

G. Security & Privacy – Security and privacy are essential challenges in today's life. Any unauthorised user can detect the data and corrupt it and change the actual data, so that receiver will get wrong data. Through neighbour identity authentication, user can verify the identity of user whether it is authorised or not.

The application of this wireless network is limited due to the mobile and ad-hoc nature. As well as, the absences of a centralized unit not allow the use of firewall. It also faces a multitude of security threats just like wired networks. That includes passive eavesdropping, denial of service, spoofing, and others. The attacks are normally categorized on the basis of applied methods and the consequences.

V. VANET VULNERABILITIES

Defencelessness is a weakness in security system [6]. A system may be vulnerable to unauthorized data handling because the system does not authenticate a user's identity before permitting data access. VANET is more vulnerable than fixed cable network. Some of the vulnerabilities are as follows:

A. Lack Of Centralized Management

VANET doesn't have a centralized governing server. The absence of administrative control create hurdle in attacks detection because it is too complex for monitoring the traffic in a dynamic and scalable ad-hoc network. Absence of centralized administration will obstruct trust management for devices.

B. Resource Availability

Resource availability is a major fear in VANET. Offering secure communication in such environment and defence against precise issues and attacks, need to enhance various security techniques and architectures. Cooperative ad-hoc network offers implementation of self-organized security.

C. Scalability

Mobility of nodes, scale the ad-hoc network all the time. Therefore, scalability is a major concern in security. Security methodologies should be capable to treat a huge network as well as minor ones.

D. Co-Operativeness

Routing algorithm for VANETs typically assume that devices are cooperative and trusted. Thus a malicious attacker can easily become an essential part or routing agent and interrupt network operation by violating the protocol conditions.

E. Dynamic Topology

Dynamic topology and changeable nodes positions may interrupt the trust management among nodes. The trust may also be an issue if a device detected as negotiated. These dynamic deeds could be better secure with distributed and adaptive security mechanisms.

F. Limited Power Supply

The nodes in mobile ad-hoc network need to consider limited power supply, which will create several issues. A node in network may act in a self-interested style, when it is concluding that there is only limited power supply.

G. Bandwidth Constraint

Variable limited capacity connections as wireless network which are more vulnerable to exterior noise, intrusion and signal weakening effects.

H. Adversary Inside The Network

The participating devices in the VANET can independently connect and leave the network. The nodes in network also act maliciously in condition of internal attacks. This is complex to find that which node is malicious. Therefore, any kind of attack is more unsafe than the external attack. These nodes are called compromised nodes.

I. No Pre-Defined Boundary

In mobile ad-hoc networks cannot specifically define a boundary of the network. The nodes act in a wandering atmosphere where they are offered to use the wireless network services. When a node is in the range that will enable it to communicate with the node. There are various kinds of attacks exist impersonation, eavesdropping, tempering, and Denial of Service attack.

VI. CONCLUSION

Recently in VANET , researcher focus towards an authentication schemes were to lower communication overhead, preserve node anonymity, isolation of misbehaving nodes, and non-repudiation. These, however, were not the only objectives stated in the following works. One keynote, is that most of the works aimed at providing various security properties which would be appropriate for one particular application or privacy level, but is more than required for another. Research directions are aimed at implementing a Trust Validation Model to reduce the vulnerability window on infrastructure-less scenarios, which includes exploring reputation based systems, and more efficient revocation information distribution mechanisms.

REFERENCES

[1] Prakashgoud Patil, Umakant Kulkarni "Svm Based Data Redundancy Elimination For Data Aggregation In Wireless Sensor Network", International Conference Of Advance In Computing Communication And Informatics, IEEE, 2013

[2] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, And Xuemin (Sherman) Shen "A Lightweight Encryption Scheme For Network-Coded Mobile Ad Hoc Networks," IEEE Trans. Parallel And Distributed Systems, Vol. 25, No. 9, September 2013.

[3] Ahmad Ali Abdullah, Lin Cai And Fayez Gebali, "Dsdmac: Dual Sensing Directional Mac Protocol For Ad Hoc Networks With Directional Antennas" ,IEEE Transactions On Vehicular Technology, Vol. 61, No. 3, March 2012

[4] Weng Chon Ao, Shin-Ming Cheng And Kwang-Cheng Chen, " Connectivity Of Multiple Cooperative Cognitive Radio Ad Hoc Networks", IEEE Journal On Selected Areas In Communications, Vol. 30, No. 2, February 2012

[5] Emiliano De Cristofaro And Claudio Soriente, "Participatory Privacy:Enabling Privacy In Participatory Sensing", IEEE Transactions On Networking Vol.27 No.1 Year 2013

[6] Quansheng Guan, F. Richard Yu, Shengming Jiang, Victor C. M. Leung, Hamid Mehrvar, "Topology Control In Mobile Ad Hoc Networks With Cooperative Communications",IEEE Wireless Communications April 2012

[7] Ajay Kushwaha,Hariram Sharma, "Enhancing Selective Encryption Algorithm For Secured Manet",2012 Fourth International Conference On Computational Intelligence, Modelling And Simulation

[8] M.Umaparvathi1, Dr.Dharmishtan K Varughese, "Evaluation Of Symmetric Encryption Algorithms For Manets", IEEE, 2010

[9] Mehta Manisha Pravinchandra, Hiteishimilinddiwanji&Jagdish And Hemali Kotak, "Performace Analysis Of Encryption And Decryption Using Genetic Based Cancelable Non-Invertible Fingerprint Based Key In Manet",IEEE,2012 International Conference On Communication Systems And Network Technologies

[10] Lin Yao, Chi Lin∗, Jing Deng, Fangyu Deng, Jingwei Miao , And Kangbinyimguowei Wu, "Biometrics-Based Data Link Layer Anonymous Authentication In Vanets"2013 Seventh International Conference On Innovative Mobile And Internet Services In Ubiquitous Computing, IEEE 2013.

[11] Riaz Ahmed Shaikh And Young-Jae Song , Hassan Jameel , Brian J. D'auriol, Heejo Lee , Sungyoung Lee, "Achieving Network Level Privacy In Wireless Sensor Networks", Sensors 2010, 10, 1447-1472; Doi:10.3390/S100301447.