NETWORK SECURITY BASED ON CHAOTIC MAPS BASED AUTHENTICATION IN VANETS

Muqtadir
Research Scholar computer science engineering Rayalaseema University
PP. COMP SCI&ENGG. 0384
Kurnool,Andhra Pradesh,India.
.
Dr. Syed Abdul Sattar
Director R & D,
Nawab Shah Alam Khan College of Engg. & Tech. (NSAKCET),
Hyderabad
. Telangana, India

Abstract: -
With an emergence of applications of Mobile Ad-hoc Networks in several areas, vehicular ad-hoc networks are constantly evolving for traffic monitoring, reducing accidents and various other applications. However, these networks are vulnerable towards malicious nodes, which might send false signals leading towards accidents causing human life and financial losses. Thus, vehicular ad-hoc networks require a faultless security approach to protect the network environment from security threats. Recently, various security methods were developed to address the security threats through cryptography. However, security methods must cause minimum overhead with respect to delay and computation, as VANET is a delay sensitive network. To assign security in any communication medium, authenticated key agreement is a precondition. Authenticated key agreement is a procedure of authenticating communicating devises by providing session keys between them. Thus, in this paper, we design a password based light weight authenticated key agreement between communicating nodes with the help of Chaotic Maps. We compare our method with RSA based authenticated key agreement protocols. Performance results shows that proposed work time complexity is less in comparison with RSA based authenticated key agreement protocols.

Key words :- Vehicular Ad-hoc Networks, authentication, security and chaotic maps.

Introduction

Vehicular Ad-hoc Networks [2] (particularly termed as VANETs) are based on the principles of Mobile Ad-hoc Networks (MANETs). These networks are particularly used to relay the information among vehicles to facilitate vehicular communications. This inter-vehicular communication aids roadside navigation, traffic monitoring, vehicular safety and other services [3]. Each vehicle establishes its data such as time, location, speed and direction at every 300ms. The data is processed between vehicles, RSUs (Road Side Units) and DMV (Department of Motor Vehicle) [4].

Generally, the vehicular information is transmitted to the other vehicles and RSUs in range. RSUs are deployed at particular distances and act as an access point to the vehicles. They send the vehicular information towards the DMV (Department of Motor Vehicles).

A VANET infrastructure has heterogeneous configuration similar to Mobile Ad-hoc Networks, where each node acts as a router and a host. It is mainly comprised of three components i.e., Vehicles, RSUs (Road Side Units) and DMV (Department of Motor Vehicles). The information is shared between these three components to keep the connection intact and secure. This network uses a radio frequency range of 5.9 GHZ based on 802.11p IEEE standard for wireless transmission.

Vehicles: The vehicles are individual nodes recorded at a centralized Department of Motor Vehicles. They share their information such as location, time and velocity with the other nodes. The vehicles are deployed with On-board units and GPS devices to connect and share the data

using 802.11p IEEE spectrum. Vehicular nodes might be either benign or malicious depending on their characteristics and activities.

RSUs (Road Side Units): These are deployed as a Wireless Access Point (AP) at a specified range on intersection such as parking lot entrance and bus stations. It works on 802.11p IEEE and provides access to the vehicles in range. RSUs check the authenticity of vehicular information and report any malicious activity to the Department of Motor Vehicles. However, RSUs are vulnerable to attacks since these are components of a heterogeneous network. Attacks on RSBs can cause severe losses since the attackers can compromise multiple vehicles in range.

DMV (Department of Motor Vehicles): DMV is a centralized authority, which monitors the vehicular records such as registrations. DMV acts as a Trusted Authority as it cannot be manipulated by a malicious node or an attacker. However, excessive transmission between DMV and vehicles can cause congestion.

Transmission of Data: At a specified interval or occurrence of particular event, vehicles broadcast their information towards the other vehicles in range and RSUs. The data includes the time t, location l and event type e along with vehicular identity i. Broadcast takes place in a predetermined interval or a specific event such that $i = (t, l, e)$. Each vehicle has its own identity as registered at Department of Motor Vehicles. The architecture of VANET is shown in figure 1.

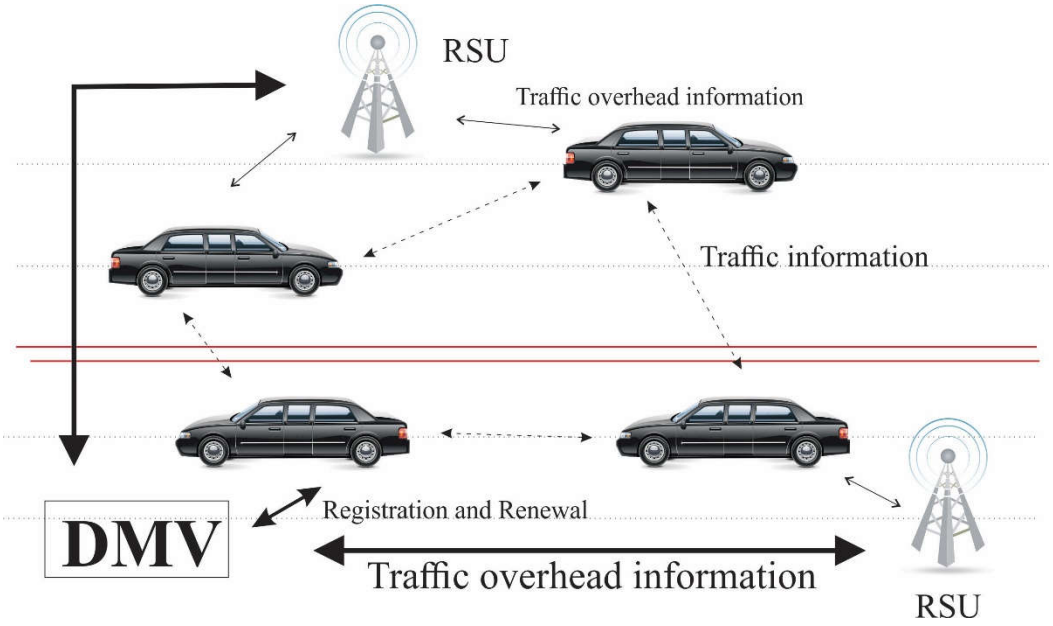

Figure 1:- Architecture of vehicular ad hoc network

VANETs use heterogeneous configuration, where each node acts as a router as well as a host. This makes communication easier between the nodes. However, it also leaves VANETs more vulnerable to threats and attacks. An attacker can be either among the nodes having access to the information or an intruder from an outside source.

The primary functions of VANETs are to prevent vehicular accidents and unnecessary traffic jams by exchanging the messages between the vehicles. VANETs also help in applications such as altering routes and avoiding collision. Due to their heterogeneity, VANETs are prone towards all the security threats affecting wireless networks. However, the security measures are different in comparison with the other wireless networks.

Some types of attacks include false information, Denial of Service (DoS), replaying events, worm hole attacks, disclosure of identity, altering messages, compromising RSB and so on.

These attacks cause severe traffic issues and accidents making human life more prone towards casualties.

Privacy must also be emphasized along with security as an intruder can have further advantage if all the vehicular information is revealed. This paper addresses various types of attacks majorly found in wireless networks.

VANETs incur various types of attacks [5] that are prominent in wireless network. These attacks are assumed according to the vulnerabilities in VANETs and the intentions of attackers. Attackers can either be among the vehicular nodes or outsiders intruding the network by compromising RSUs or other vehicles.

Vehicular Data Manipulation: An attacker collects the vehicular data from a transmitting node, modifies the information and forwards to the other nodes.

False Sensor Information: An attacker broadcasts false information to the nodes in a range to affect the behavior of drivers in order to cause accidents.

Replaying Packets: In this case, an attacker collects an event from the other nodes and replays the same in different locations and timestamps.

Denial of Service (DoS) attacks: These are severe types of attacks where an attacker causes congestion in central mediums such as RSUs. They proceed their attacks on the other nodes by averting the access to the medium.

Distributed Denial of Service (DDoS) attacks: These attacks are more severe than DoS attacks where an attacker uses several vehicular identities and sends the messages from different timestamps and locations.

Mimicking Nodes: In this case, an attacker uses the identity of other nodes to mask and sends the wrong information on behalf of those nodes.

Delay in Messages: An attacker adds timestamp to an original message such that it causes delay in receiving of message.

Sybil Attacks: In these attacks, an attacker uses an identity of different vehicles and sends multiple messages to the nodes.

Providing security and mitigation attacks in VANET is a vital issue. In order to incorporate security in any network environment easy and simple way is to provide mutual authentication [1] between communicating nodes/ devices. Thus in this paper we design the light weight password based authenticated key agreement between communicating nodes. The detail discussion of proposed protocol is available in following sections.

Mitigation of Malicious Attacks on VANETs using Chaotic Maps

Various malicious attacks can be prevented by recognizing the behavior and activity of an attacker. The types of attacks and intentions of attackers were assumed from the related work based on security of Wireless Networks.

Most of the attacks can be caused by disclosure of vehicular identities and messages. Since the messages between the nodes are sent in a plaintext form, attackers can easily manipulate the information once they intrude the network. To prevent these attacks, authenticated key agreement is helpful where messages between the source and the destination are encrypted. This work is based on chaotic maps based authenticated key agreement. In this scheme, each node requires a password to send messages to the other nodes.

Initially we computed the time complexity of chaotic map based and modular arithmetic based Diffie Hellman key exchange problem. The Sequence of steps for chaotic map based based Diffie Hellman key exchange problem as follows.

1. The Source and The Destination agree upon a specific Prime number, let X.
2. The Source computes the value of $T_n(X)$ using the following equation, by considering a large prime number 'n'.

$T_n(X)$ =2 *X*$T_{n-1}(X)$ - $T_{n-2}(X)$

3. The Source sends the computed value $T_n(X)$ towards the destination.
4. The destination in turn computes the value of $T_m(X)$ using the following equation, by considering a big prime number 'm'.

$T_m(X)$ =2 *X*$T_{m-1}(X)$ - $T_{m-2}(X)$

5. Then the destination sends the computed $T_m(X)$ value towards source node.
6. Further, the destination computes the value of $T_{mn}(X)$, with the help of a received value by the following equation.

$$T_{mn}(X) = T_m\big(T_n(X)\big)$$

7. Then, it sends the computed $T_{mn}(X)$ value back to the source node.
8. Source node validates the received value $T_{mn}(X)$ by calculating the value of $T_{nm}(X)$ by following equation.

$$T_{nm}(X) = T_n\big(T_m(X)\big)$$

Secondly we computed the time complexity of modular arithmetic [8] based Diffie Hellman key exchange problem. The Sequence of steps for modular arithmetic based Diffie Hellman key exchange problem as follows.

1. The Source and The Destination agree upon two big prime numbers i.e., P, N.
2. The Source computes the value 'J' using below equation by selecting a prime number 'A'

$$J = N^A \ mod \ P$$

3. The Source sends the value J towards the destination node.
4. The destination node computes the value 'K' using the following equation by selecting a prime number 'B'.

$$K = N^A \ mod \ P$$

5. Destination send the value J towards the source node.
6. Now, the source computes the value $K^A \ mod \ P$.
7. The destination also computes the value of $J^B \ mod \ P$.
8. The values calculated by the source as well as the destination are ensured to match.

Performance analysis of RSA and Chaotic Maps based Diffie Hellman key exchange Problem in a static identical condition

The performance of RSA [7] and Chaotic maps [6] based authenticated key agreement is evaluated based on static identical states. For performance evaluation, network simulator NS2.35 [9] is used. The hardware specifications comprised a Hard Disk of 160 Gigabytes capacity, DDR2 SDRAM with 2GB memory and clock rate of 667MHz, Dual Core 2.33 GHz processor with 2MB Cache. The computation time is evaluated for each algorithm in identical conditions. Results are shown in figure 2 and 3.

The results demonstrate that the computation time taken by Chaotic Maps is far less in comparison with RSA based authentication. Furthermore, reduction of computational time increases the network performance, occupies less buffer and consumes less energy. Chaotic maps induced less overhead on VANETs in comparison with RSA.

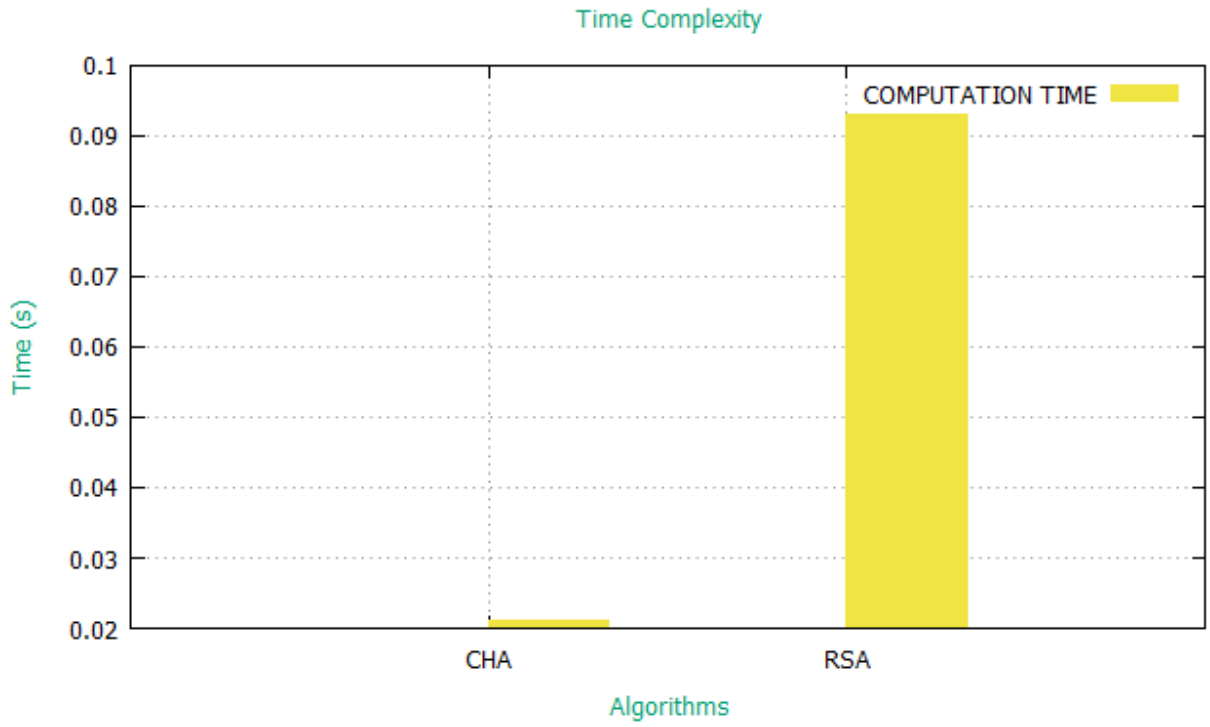

Figure 2 :- Comparison of RSA and Chaotic maps in static identical environment

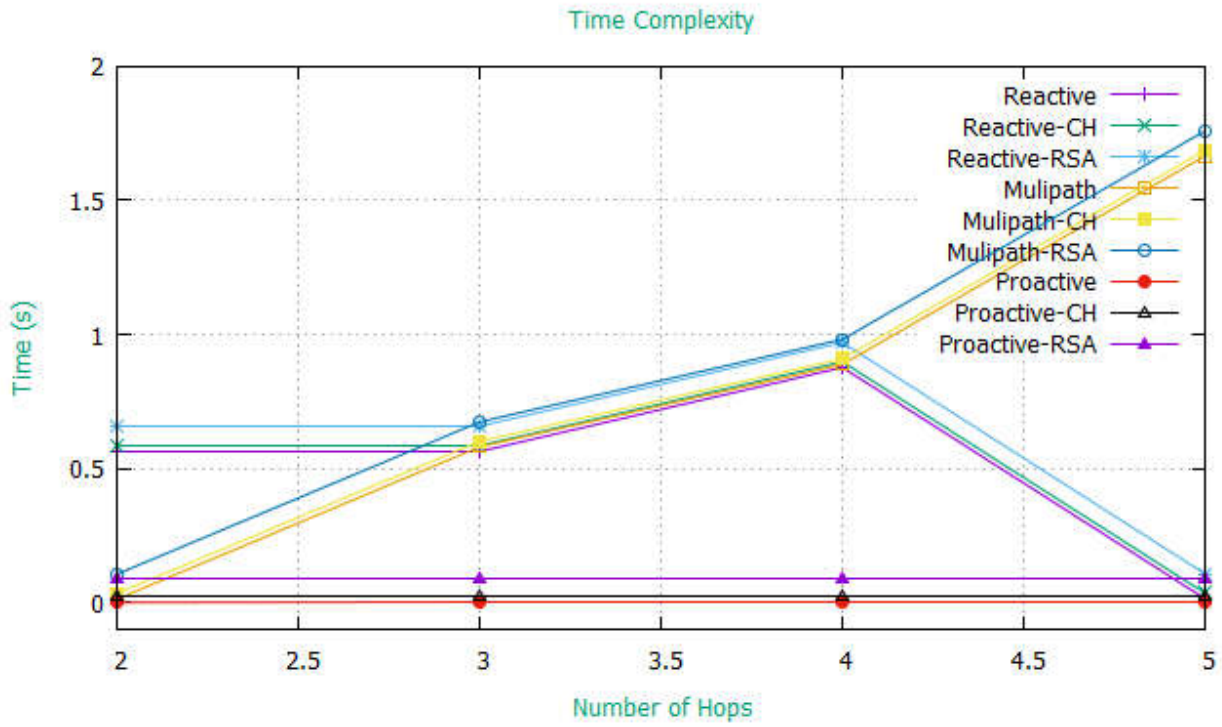

Figure 3:- Comparison of RSA and Chaotic maps in dynamic identical environment

Proposed password based Authenticated key agreement based on Chaotic maps

Proposed algorithm, i.e., password Authenticated key agreement based on Chaotic maps between two vehicles are explained as follows

1. The Source and The Destination agree vehicles upon a specific Prime number, let X.
2. The Source vehicle computes the value of $T_n(X)$ using the following equation, by considering a large prime number 'n'.

$T_n(X)$ =2 *X*$T_{n-1}(X)$ - $T_{n-2}(X)$

3. The Source select a password and compute the following value

$$Tuple = (T_n(X) \,||\, ID_s \,||\, ID_D \,||\, Password)$$

4. Source vehicle calculate the hash value of tuple

5. $Digest = H(T_n(X) \,||\, ID_s \,||\, ID_D \,||\, Password)$
6. The source sends the $\{T_n(X),\ Password,\ Digest\ \}$ towards the destination.
7. The destination in turn computes the value of $T_m(X)$ using the following equation, by considering a big prime number 'm'.

$T_m(X)$ =2 *X*$T_{m-1}(X)$ - $T_{m-2}(X)$

8. The destination select a password and compute the following value

$$Tuple = (T_m(X) \,||\, ID_s \,||\, ID_D \,||\, Password)$$

9. Destination vehicle calculate the hash value of tuple
10. $Digest = H(T_m(X) \,||\, ID_s \,||\, ID_D \,||\, Password)$
11. The destination sends the $\{T_m(X),\ Password,\ Digest\ \}$ towards the destination.
12. Further, the destination computes the value of $T_{mn}(X)$, with the help of a received value by the following equation.

$$T_{mn}(X) = T_m\big(T_n(X)\big)$$

13. Then, it sends the computed $T_{mn}(X)$ value back to the source node.
14. Source node validates the received value $T_{mn}(X)$ by calculating the value of $T_{nm}(X)$ by following equation.

$$T_{nm}(X) = T_n\big(T_m(X)\big)$$

In the above algorithm source and destination vehicles are validate the received values by comparing the received digest values.

Conclusion:

VANETs use heterogeneous infrastructure based on MANETs, which leaves VANETs more vulnerable to security issues. To prevent these issues, a chaotic maps based algorithm is

used based on Public Key Cryptography. This digested the messages sent between the nodes and thereby prevents attackers using chaos method. The Chaotic Maps based algorithm has been compared with RSA based algorithm in an identical environment, which concludes that Chaotic Maps based encryption induces less overhead when compared to RSA based encryption. Moreover, Chaotic Maps is a lightweight algorithm causing less consumption of memory, bandwidth and energy, which prevents congestion due to overhead. Hence, this paper concludes that Chaotic Maps based authentication is a lightweight and strong cryptographic technique to prevent security holes in VANETs.

References

1. Memon, I., 2015. A secure and efficient communication scheme with authenticated key establishment protocol for road networks. *Wireless Personal Communications*, *85*(3), pp.1167-1191.
2. Mukherjee, J.C., Agarwal, S. and Gupta, A., 2014, May. Distributed event notification in VANET with multiple service providers. In *Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems* (pp. 334-337). ACM.
3. Chen, Z., Liu, Y., Wong, R.C.W., Xiong, J., Mai, G. and Long, C., 2014, June. Efficient algorithms for optimal location queries in road networks. In *Proceedings of the 2014 ACM SIGMOD international conference on Management of data* (pp. 123-134). ACM.
4. Wang, Y. and Li, F., 2009. Vehicular ad hoc networks. In *Guide to wireless ad hoc networks* (pp. 503-525). Springer, London.
5. Al-Kahtani, M.S., 2012, December. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on* (pp. 1-9). IEEE.

6. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. *Indian Journal of Science and Technology*, *9*(26).
7. Eissa, T., Razak, S.A. and Ngadi, M.D., 2011. Towards providing a new lightweight authentication and encryption scheme for MANET. *Wireless Networks*, *17*(4), pp.833-842.
8. Ovshinsky, S.R. and Pashmakov, B., Energy Conversion Devices Inc, 2004. *Methods of factoring and modular arithmetic*. U.S. Patent 6,714,954.
9. Issariyakul, T. and Hossain, E., 2012. Introduction to Network Simulator 2 (NS2). In *Introduction to Network Simulator NS2* (pp. 21-40). Springer, Boston, MA.