International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 6, June 2015)

Secure Trajectory Based Data Delivery in VANETS

Abishek N L
Digital Communication & Networking
Dayananda Sagar College of Engineering
Bangalore, India.
currentabs@gmail.com

Mrs. P. Rajeshwari
Digital Communication & Networking
Dayananda Sagar College of Engineering
Bangalore, India.

***Abstract*— Secure and Efficient data delivery plays very importance role in vehicular networks, but highly challenging of frequent network interruption, fast topological changes and also the attackers in the network. The Data Storage‘s attack is a severe attack that can be easily launched by a pair of external attackers in Networks. In this attack, an attacker sniffs packets or data at one point in the network by injecting fake contents or wrong data for corresponding nodes. In this paper, the system proposes novel attackers detection and positioning scheme based on mobile Location Based Server, which can not only detect the existence of Network Node attacks, but also accurately localize the attackers for the system to eliminate them out of the network and enhancing the digital signature value using Secure Hash Algorithm – 512 due to security reason.**

***Index Terms*— Vehicular networks , Trajectory, Routings, Server Provider ,VAN Router .**

I. INTRODUCTION

Vehicular network is a network of vehicles which communicate with each other via short-range wireless communications. Vehicles can therefore communicate with each other directly when they meet each other or through multihop transmissions. Vehicles can act as powerful sensors and form mobile sensor networks. Vehicular networks have many appealing applications such as driving safety , intelligent transport , infra-structure monitoring and urban monitoring. 3G networks are more popular and access to 3G is possible in urban vehicular network. Moving vehicles can also communicate with each other via 3G.However communication via 3G has limitation. The cost of 3G communication is very high compared to ad hoc vehicular communication which is for free and also the bandwidth of inter-vehicle communication can be higher than that of 3G. Finally, many real-time applications are time critical so ADHOC networks are more suitable

Efficient and secure inter-vehicle data delivery is of central importance to vehicular networks . In this paper focus is on such vehicular networks that are sparse and do no assume that all vehicles on the road are member nodes of the vehicular network. In Such sparse vehicular networks feature the infrequent communication opportunities and Inter-vehicle data delivery may introduce non negligible delivery latency because of frequent topology disconnection of a vehicular network. Thus should stress that the inter-vehicle communication in vehicular network are suitable for those applications which can tolerate certain delivery latency.

There is a great deal of uncertainty associated with vehicle mobility. Vehicles move at their own wills. It is difficult to gain the complete knowledge about the vehicular trace of future movement, i.e., the position of the vehicle at a given point in time. For routing in a vehicular network a relay node must decide how long a packet should be kept and which node a given packet should be forwarded to. Existing study shows that it is possible to find an optimal routing path when the knowledge of future node is Known. Networks is the one of the areas in the field of wireless communication, where in delay is particularly high. They are promising technology in vehicular, disaster response, under water and satellite networks. Delay tolerant networks are characterized by large end to end communication latency and the lack of end to end path from a source to its destination and they pose several challenges to the security of WSNs. In the network layer there are many attacks so we consider most common types of attacks on these networks. With the help of these attacks they give serious damages to the network in terms of latency and data availability. Using entropy anomaly detection algorithm motivated by the detection of external attackers and to prevent them from the attacking data from the outside environment.

Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed hash to a known and expected value of hash, the data's integrity can be determined. For example, computing the hash of a downloaded file and by comparing it to previously published hash result can show whether the download has been modified or tampered with.

The SHA512 algorithm is very similar to SHA256, and most of the general optimization principles described in this system apply here as well. The main differences in the algorithm specification are that SHA512 uses blocks, digests and data-type of computation twice the size of SHA256. In addition, SHA512 is specified with a larger number of rounds of processing.

II. SYSTEM ARCHITECTURE

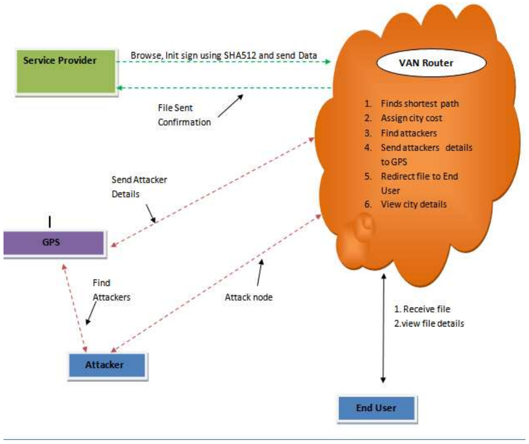


Fig.1. Architecture for Secure Data Delivery in Vanet's

Data Service provider:

In this module, the data service provider will browse the data files available and initialize the nodes, then select a node & send to the particular end user. Data Service provider will send their data file to VAN router and in a VAN router less cost node will select and send to the particular end user. After receiving successful the data provider will get response from the router.

VAN Router

In this module, the VAN router consist of n-number of nodes to provide a data service. The VAN router will receive the data file from the service provider and select a less cost node and send to the particular end user. If any attacker will found in a router, then the VAN router will select another less cost node and send it to the end user. Van router can assign city cost, view city details and view attackers. If city cost has to be assigned, then select city name and enter new cost and submit, then it will be stored in a VAN router.

GPS

In this module, some operation such as view vehicle trajectory and view attack destination are done. If we select view vehicle trajectory, then all information about vehicle with their tags such as city name, metadata, date & time is received. In GPS the details of the attacker can be viewed with their tags such as attacker name, city name, Mac address, time and date.

End User

In this module, there are n-number of end users are present (A, B, C and D). The end user can receive the data file from the service provider via VAN router. The end user will receive the file by without changing the File Contents. Users may receive particular data files within the router only.

Attacker

Attacker is one who is rerouting the trajectory node. The attacker will select the node and inject fake key to the particular node. After attacking successful the attacker details will store in GPS and VAN router with their tags such as attacker name, city name, IP address, time & date.

III. PROPOSED METHODOLOGY

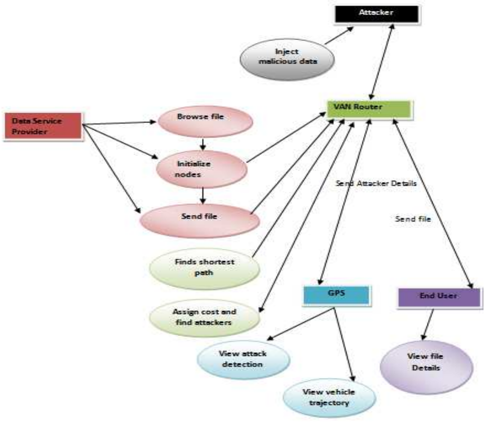
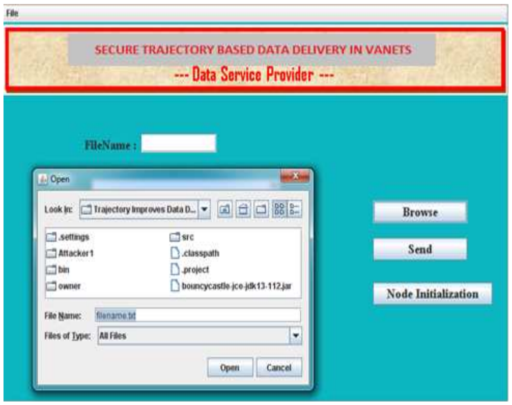


Fig 2. Methodology Used

The proposed methodology uses the following modules given below.

- The data service provider browses the data file and initialize the nodes, then select a node & send to the particular end user.
- Data Service provider will send their data file to VAN router and in a VAN router less cost node will select and send to the particular end user.
- The sent data will have a Cryptographic Hash function SHA512 which provides the Security against the Attackers in the network.
- The VAN router consist of n-number of nodes (A, B, C, D, E and F) to provide a data service.
- The VAN router will receive the data file from the service provider and select a less cost node and send to the particular end user.
- If any attacker will found in a router, then the VAN router will select another less cost node and send to particular end user.
- In a VAN router we can assign city cost, view city details and view attackers.
- In GPS some operation such as view vehicle trajectory and view attack destination can be done.
- If we click on view vehicle trajectory, then we will get all information about vehicle with their tags such as city name, metadata, time & date.
- There are n-number of end users are present (A, B, C and D). The end user can receive the data file from the service provider via VAN router.
- The end user will receive the file by without changing the File Contents. Users may receive particular data files within the router only.
- Attacker is one who is rerouting the trajectory node. The attacker will select the node and inject fake key to the particular node.
- The Attributes are Vehicular networks, probabilistic trajectory, routing, prediction, Markov chain, File Management, data provider, end user, Attackers.

IV. RESULTS



SECURE TRAJECTORY BASED DATA DELIVERY IN VANETS

--- Data Service Provider ---

Fig 3. Data service provider Module Details

In this module, the data service provider browses the file that has to be sent to a particular destination when an user requests for a particular file and then the service provider initialises all the nodes. The IP address is then selected and also the city to which the file has to be sent is selected and the file is sent to Van router.

Before Sending the data file a Cryptographic hash function SHA 512 is added to the file to provide security against attackers in the network .

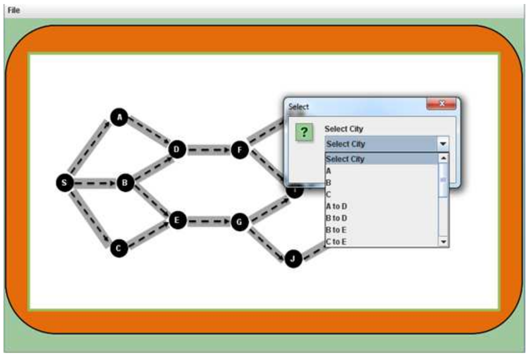
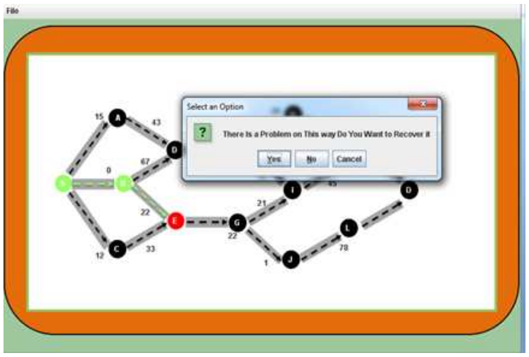


Fig 4. Van Router Module

The file that is sent by the service provider is received by the Van Router which Assigns cost to all the nodes in the networks. Then the Van router tries to find the Shortest path in the network to send the file to the Destination.



Select an Option

There Is a Problem on This way Do You Want to Recover it

Fig 5.Atacker in Van Router Module

The Data Storage‘s attack is a severe attack that can be easily launched by a pair of external attackers in Networks. In this attack, an attacker sniffs packets or data at one point in the network by injecting fake contents or wrong data for corresponding nodes. The attacker in the network who intends to modify the data will select a particular node and injects fake key into that node. In GPS, the Details of the attacker can be viewed with their tags such as attacker name, City name , MAC address, Date and time .

we can see in the figure above where a fake data is injected in the node C. when the van router is sending the data from source node to the destination node it finds out that there is an attacker at node c. so it tries to recover the path that has been attacked or it tries to find another shortest path in which the required data can be sent to the destination.

Conclusion

In the network layer there are many attacks so most common types of attacks on these networks can be considered. With the help of these attacks they give serious damages to the network in terms of latency and data availability.

In this paper, the system proposes novel attackers detection and positioning scheme based on mobile Location Based Server, which can not only detect the existence of Network Node attacks, but also accurately localize the attackers for the system to eliminate them out of the network. A cryptographic hash function SHA 512 is used in the Service Provider modules which helps to prevent the attackers in the network in the Van Router module and helps in sending the data file from source to destination in a secure manner.

REFERENCES

[1]. z. Li, Y. Liu, M. Li, J. Wang, and Z. Cao, “Exploiting Ubiquitous Data Collection for Mobile Users in Wireless Sensor Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 2, pp. 312-326, Feb. 2013.

[2]. M. Li and Y. Liu, “Rendered Path: Range-Free Localization in Anisotropic Sensor Networks with Holes,” IEEE /ACM Trans. Net-working, vol. 18, no. 1, pp. 320-332, Feb. 2010.

[3]. J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan , “The Pothole Patrol: Using a Mobile Sensor Net-work for Road Surface Monitoring,” Proc. ACM Sixth Int’l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.

[4]. A. Balasubramanian, B. Levine, and A. Venkataramani, “DTN Routing as a Resource Allocation Problem,” Proc. ACM SIG-COMM, 2007.

[5]. L. Chisalita and N. Shahmehri, “A Peer-to-Peer Approach to Vehicular Communication for the Support of Traffic Safety Applications,” Proc. Fifth IEEE Conf. Intelligent Transportation Systems, pp. 336-341, 2002.