ISSN: 2321-7782 (Online)
Volume 2, Issue 8, August 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Holistic Protocol Based Outsider and Insider Attack Detection in VANET Multihop Data dissemination Protocol – a Survey

G.Gayathri[1]
Research Scholar
Department of Computer Science
Sri Krishna Arts and Science College
Coimbatore – India

D.Shona[2]
Assistant Professor
Department of Management Studies
Sri Krishna Arts and Science College
Coimbatore – India

Abstract: ***Vehicular ad hoc networks (VANETs) use the vehicles as nodes to communicate between the nearby vehicles. It can be used to inform about the traffic, road conditions and accidents which helps to improve road safety and traffic efficiency. Multi-hop data dissemination protocol is used to detect the insider attack and improve security. In order to improve the security HOLISTIC PROTOCOL has been developed. This simulation result shows that the scheme highly detects and avoids the insider/outsider attack.***

Keywords: VANET, Attacks in VANET, Multihop data dissemination protocol, Holistic protocol.

I. INTRODUCTION

A **vehicular ad hoc network (VANET)** uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. This technology is applied in police vehicles and fire.

The main benefit of VANET communication enhancement of passenger safety by exchanging warning messages between vehicles. The growth of the increased number of vehicles is equipped with wireless services in order to communicate with other vehicles to form a special class of wireless networks.

One of the most used concepts to support communication in VANET is IPv6. It is used to allocate the IP addresses to all other devices and it extended address space, embedded security, enhance the mobility support and ease of configuration in VANET.

Attacker creates a problem in the network by getting full access of communication medium. There are various types of possible attacks on VANETs. Insider attack might access to knowledge will be use for understanding the design and configuration on network. When they have all information about the configuration then it is easy for them to launch attacks. It can create a problem in the network by changing the certificate keys.

The outsider attack is considered as an authentic user of the network. It is a kind of intruder which aims to misuse the protocols of the network. Outsider attack also has limited diversity for launching different kind of attacks.

II. Related Work

The dynamics of the network due to vehicle movement further complicates the design of an appropriate comprehensive communication system. Collect and categorize envisioned applications from various sources and classify the unique network characteristics of vehicular networks. Based on this analysis, consider five distinct communication patterns that form the basis of all VANET applications. Both the analysis and the communication patterns shall deepen the understanding of VANETs and simplify further development of VANET communication systems [1].

The range of mechanisms, to handle identity and credential management this is used secure communication while enhancing privacy. In this contribution, the problem discuss implementation and performance aspects, present a gamut of research investigations and results towards further strengthening secure VC systems and addressing remaining research challenges towards further development and deployment of our architecture[2].

To motivate the deployment of a security system for a vehicular environment is different compared to other common information technology systems. The VC security mechanisms should be flexible, adaptable, and extensible, to allow later adjustments to changing security requirements. To address this need, propose component-based security architecture for VC systems, which allows adding, replacing, and reconfiguring components (for example, substitute cryptographic algorithms) throughout the life cycle of the vehicle [3].

Safety applications that try to make driving safer, e.g., road hazard warning; traffic efficiency applications aiming at more efficient and thus greener traffic, e.g., detection of traffic jams; manufacturer oriented applications, e.g., automatic software updates; and comfort and entertainment applications, e.g., automatic map updates or video streaming[4]. Nodes either comply with the implemented protocols or they deviate from the protocol definition and become adversaries. The attacks that can be mounted by either internal or external adversaries vary greatly. In brief, adversaries can replay any message, jam communications, and modify messages [5].

Parsimony assumes that an attack involving a few malicious nodes is more likely than an attack that requires collusion between a large numbers of nodes. Malicious node can create additional fictitious nodes to bolster its view of the VANET. This is known as a Sybil attack [6]. One way to implement data consistency checking is to exploit redundant information dissemination to detect inconsistencies. Numerous protocols have to provide the necessary information dissemination [7].wireless Multihop network is minimum node degree and its *k*–connectivity [8]. A path redundancy based security algorithm (**PRSA**) to improve routing security in wireless sensor network. The algorithm uses alternative routing paths for each data transmission call to overcome the sensor network attack [9]. One key objective in the topology design of a WSN is to ensure some measure of robustness. to ensure routes to the sink are available for all remaining sensor nodes after the failure of up to k ▪ 1 nodes. This can be achieved by ensuring that every node in the initial design has k node-disjoint paths to the sinks: i.e. at least k paths that share no intermediate nodes. Node-disjoint paths are required to provide multi-path routing capability for some protocols [10].

The main objective is to detect insider and outsider attack and provide a alternative path for an data transmission and then to develop a holistic protocol.

III. Attacks in VANET

In Many of attacks against VANETs have emerged recently that attempt to compromise the security of such networks. Such security attacks are as follows,

3.1 Insider Attack:

An insider attack is a malicious attack on a network or computer system by a person with authorized system access. Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and

also may be familiar with network architecture and system policies/procedures. Insider attacks are less security because many organizations focus on protection from external attacks.

3.2 Outsider Attack:

The intruder is someone who has been entrusted with authorized access to the network.

3.3 Denial of Service attack:

This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving.

3.4 Message Suppression Attack:

An attacker can select and dropping packets from the network.

3.5 Fabrication Attack:

An attacker can make this attack by transmitting false information into the network,

3.6 Alteration Attack:

This attack happens when attacker alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted.

3.7 Replay Attack

This attack happens when an attacker replay the transmission of earlier information to take advantage of the situation of the message at time of sending. It does not contain sequence numbers or timestamps. Individual Packets must be authenticated, not just encrypted. Packets must have timestamps.

3.8 Sybil Attack:

This attack happens when an attacker creates a large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route.

IV. PREVIOUS SYSTEMS

Attackers can generate wrong information or modify information they process as part of multi hop dissemination protocols. Hence, cryptographic signatures cannot guarantee that messages contain correct information. This problem is worse in multi hop protocols. If geo-cast is used to forward messages over large distances, it is likely that the receivers of messages do not have any previous interactions with originators of messages. Entity centric trust with data-centric methods, which detect attacks based on data consistency rather than entity trust. The central idea is to rely on physical models, local sensors, or data redundancy to detect spurious data. The method data transferred using piggybacking, and the insider attack is detected using multi-hop data dissemination protocol and then an alternate route is made available using self reconfigurable technique through which the data are transferred in secure.

4.1 Data Consistency:

Different data consistency approaches for VANETs. Among these, identify redundancy as a promising approach particularly for Multihop protocols. Representing a message transfer of a Multihop protocol as a directed graph, derive metrics to assess communication redundancy. The goal is to analyze whether redundancy can be exploited to achieve data consistency in multihop dissemination protocols.

Contributions can be summarized as follows.

- Categorize approaches for data consistency and assess their applicability to Multihop data dissemination.
- Propose graph-based metrics to gauge data redundancy in data dissemination protocols.
- Perform extensive simulations using existing protocol proposals to validate our metrics and to discuss whether data redundancy is a valid approach for future data centric integrity protection methods

This process has some disadvantages like packet drop. To overcoming the drawbacks go for holistic protocol. By which both insider & outsider attacks are detected and avoided for enhance the network security. The holistic protocol will be implemented with probabilistic approaches. Generally in other vehicle to vehicle communication system, the node will be disseminating the data with or without request.

V. PROPOSED STUDY

The holistic approach of VANET is formulated in order to rectify the disadvantages of the existing system and to improvise the security level of data communication in the VANET. This system is designed through various benchmarks. They are Mobility and Authentication, Verification of Data Consistency and Message Integrity, Parametric check, Outsider and Insider Attack Detection.

VI. SYSTEM ARCHITECTURE

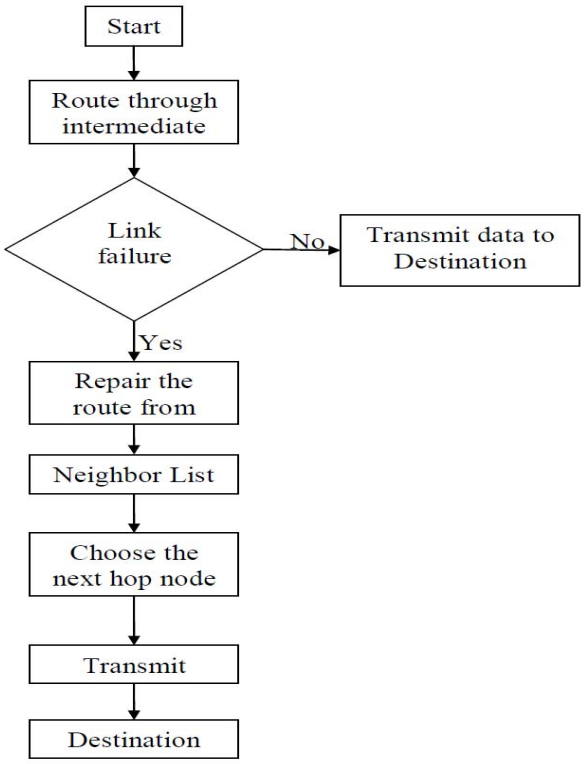

Fig.1

This study is basically without infra-structure support. Mobility is done in slow interval. The defined position explains specification on the node for its communication space and assigns the communication node. When the nodes are in moving state, a communication distance will be generated which is approximately 500 meters. Within This communication distance any node can communicate to any other node or nodes.

Message integrity is formulated through broadcast interval. Broadcast interval defines the time taken to communicate a message and time gap after communication. Normally this interval is assigned as 20 seconds for a communication between the nodes. Here in this communication maximum 750 nodes to minimum 100 nodes can make communication. In the case communication, the node gets an interval gap as a delay for its reply transmission (i.e. a vehicle sends a data and gets some delay for its reply). Here transmission power is very essential. This is for defining the kind of network for communication and communication standard. In this communication is also done between disjoint paths of nodes in the communication networks. Communication standard is when a data is transmitted during the node is not in rest.

In this module protocol specific parameters are verified. The protocol specific parameters in this system are packet size, redundancy, vehicle density. Packet size is the density of the data in communication. Redundancy check is to avoid the repetition of same data in the communication and it exempts the redundant data. Vehicle density is categorized based on simulation/assumption based system and aggregation based system.

Malicious node is to be detected for the initial attack detection. For this reason, two nodes that are not in the communication distance are introduced. These two nodes follow the process of communication in the network by gathering information about the network in a short duration. After the observation it starts attacking by entering into the network and it integrates into the network. This attacker node either fetches the information from other node or indulges its information into other node in order to make attacking communication. At this point of time the holistic protocol detects this node by comparing with past database of the network nodes and it name this node as outsider attacker node. After the name tag is given to this node it is removed from the network. In case of insider attack, the node will be within the network and it is an authenticated node. This node is detected when a node inside the network trying to access the other nodes beyond its permission or provision. Here the holistic protocol identifies this node and names as insider attacker node. After naming other nodes gets detached from this insider attacker node and this insider attacker node is get removed from the network.

Hence a holistic protocol will use both absolute cryptographic security measures and probabilistic approaches together to ensure data consistency and protect future VANETs against outsider and insider attackers.

VII. CONCLUSION

Safety and security is getting a necessary for VANET applications. As VANET they use wireless technology and it is dangerous to many attacks. In this paper, proposed lightweight holistic protocol for secure data transmission against insider and outsider attacks. In this the data which transmitted securely and the misbehaviours also detected successfully. A holistic protocol will use both absolute cryptographic security measures and probabilistic approaches together to ensure data consistency and protect VANETs against outsider and insider attackers. . In future, have to implement this protocol and discuss the results.

References

1. E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, “Communication patternsin VANETs,” IEEE Commun. Mag., vol. 46, no. 11, pp. 119–125, Nov. 2008.
2. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger,M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure vehicular communication systems: Design and architecture,” IEEE Commun. Mag.,vol. 46, no. 11, pp. 100–109, Nov. 2008.
3. F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch,B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, andJ.-P. Hubaux, “Secure vehicular communication systems: Implementation, performance, and research challenges,” IEEE Commun. Mag., volume. 46, no. 11, pp. 110–118, Nov. 2008.
4. F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof, “Executive summary—Inter-vehicle communication,” in Proc. Dagstuhl Semin. 10402—Inter-Veh. Communication, Wadern, Germany, Oct. 2010.
5. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, IEEE Std.1609.2-2006.
6. M. Raya, P. Papadimitratos, V.D. Gligor, and J.-P. Hubaux, “On data centric trust establishment in ephemeral ad hoc networks,” in Proc. 27th Conf. IEEE INFOCOM, 2008, pp. 1238–1246.
7. S. Dietzel, J. Petit, F. Kargl, and G. Heijenk, “Analyzing dissemination redundancy to achieve data consistency in VANETs (short paper),”in Proc. 9th ACM Int. Workshop Veh. Inter-Netw., New York, 2012,pp. 131–134.

8. C. Bettstetter, "On the minimum node degree and connectivity of a wirelessmultihop network," in Proc. 3rd ACMInt. Symp. Mobile Ad Hoc Netw. Computer, 2002, pp. 80–91.

9. S. Al-Wakeel and A.-S. Sa, "PRSA: A path redundancy based security algorithm for wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007, pp. 4156–4160.

10. L. Sitanayah, K. Brown, and C. Sreenan, "Fault-tolerant relay deploymentfor k node-disjoint paths in wireless sensor networks," in Proc. IFIP WD, Oct. 2011, pp. 1–6.

AUTHOR(S) PROFILE

GAYATHRI.G Graduated from the Anna University M.Sc Computer Technology in 2013. She is currently doing M.Phil in Sri Krishna Arts and Science College. Published various national and international conferences.

SHONA.D MCA.,M.Phil.,MBA., B.ed working as a assistant professor at sri Krishna college of arts and science has 11 years of experience in teaching..Security in computing is her area of interest.

