A NOVEL PROTOCOL ANALYSIS FOR DATA CONSISTENCY USING GRAPH THORY IN VANET MDDP

Lavanya.R, PG Scholar,Kavitha.V M.E., Associate professor
Dept of CSE. Sri Sairam Engineering College,
Chennai-44,Tamilnadu,India.
lavanya.sairam1214@gmail.com
kavitha.cse@sairam.edu.in

ABSTRACT:

Vehicular Ad-hoc Network (VANET) represents a demanding class of mobile ad-hoc networks that enables vehicles to intelligently communicate with each other and with roadside infrastructure. It has a number of challenges in terms of Quality of Service (QoS) and its performance. Quality of Service depends on numerous parameters such as bandwidth, packet delivery ratio, data attacks, delay variance, etc. we focus on packet delivery by considering the insider attacker possessing valid key material. In order to identify and eradicate the insider attacker, we need to consider data-centric trust in that data redundancy method can be used to detect spurious data. Among several data consistency approaches the redundant information dissemination is best suited for multihop protocols, If information is come from both straightforward and malevolent vehicles, then spurious information from attackers can be identified and eliminated .Three graph-based metrics are used to estimate the redundancy of dissemination protocols, results shows that Advanced Adaptive Geocast protocol and aggregation protocols provides data consistency mechanisms that build on redundancy are probabilistic rather than absolute, here we use holistic protocol to provide absolute cryptographic security measures to ensure data consistency and protect against future attackers.

Index Terms- Data consistency, graph theory, protocol analysis, redundancy, QoS, vehicular networks(VANETs).

I.INTRODUCTION

Now a days ,vehicular ad-hoc networks are used widely in variety of applications such as safety applications, traffic efficiency and infotainment services. Safety applications is to reduce the number of injuries and fatalities of road accidents, Traffic efficiency applications intend to optimize the traffic flow on roads, i.e. minimizing the travel time by disseminating information about traffic flow conditions on roads and infotainment applications provide communication services like entertainment, web access and advertisement. Examples are remote vehicle diagnostics, video streaming, and map download for the navigation system. VANETs provide communication between the vehicle nodes and vehicle nodes to road side unit by exchanging important information, e.g., about road conditions and hazardous situations, etc., Moreover, such information can be propagated via multiple hops, thus making the dissemination of important information possible over longer distances.

Numerous protocols are exits for efficient information dissemination via multiple hop, two major dissemination patterns are Geocast and aggregation. geographic broadcast (GeoCast) disseminates information in a geographical region, information is either forwarded toward the destination region or disseminated directly. It is used by many applications to enhance traffic safety and efficiency but it can also serve as a basic mechanism for other routing protocols example use case are dissemination of emergency vehicle warnings to approaching vehicles and disseminating accident warnings. Aggregation is a communication paradigm that has the potential to enhance the scalability of multi-hop communication and, by reducing the required bandwidth per application, enable the coexistence of different applications in the same network. data items from multiple messages can be combined into one aggregated message and information is modified while it is forwarded in the network. Example use cases are traffic information systems and parking spot availability information. Communication is established by using the above dissemination protocols. While disseminating the information there is a chance of getting information from malicious vehicle. In order to prevent spreading of information from malicious vehicles all protocols should

be properly secured. Otherwise, attacker vehicles could be able to reroute traffic if they insert malicious messages into traffic information systems, for instance. In cases of safety applications, attackers could be able to cause accidents due to false information, in the worst case.

Former system they use entity centric trust which is established by providing digital signatures along with each packets by using public key infrastructure (PKI) that issue certificates to each vehicle to ensure the originators of the messages are authorized to participate in vehicular networks. Attacks using arbitrary commodity vehicles are dissatisfied. In this case knowledgeable attackers will be able to access a valid key material in vehicles, using that keys attacker can generate wrong information or modify the information .hence there is no guarantee that the signed messages will have correct information. since it is a dynamic network the originator of the message is no longer be identified.

Therefore in the proposed system Data consistency checks are used to detect attacks from insiders that posses a valid key material. It relay on multiple sources of information to detect inconsistencies between different suspected information items. The detection of inconsistencies can be used as a source for mechanisms that filter wrong information and exclude attacker vehicles from the network. We distinguish three main types of sources for data consistency mechanisms .Physical Models can be used to compare claimed information against known models, such as the physical behavior of vehicles. For instance, vehicles cannot accelerate arbitrarily fast and cannot move at infinite speed. it create a model of the VANET, which captures all possible events and uses their statistical properties to detect spurious information. Local sensors can be used to verify information received from vehicles in the direct vicinity. In case of conflicts between the perceived environment and information from other vehicles, precedence can be given to local sensor information. it uses sensors to analyze vehicle behavior and check position information. Dissemination redundancy deliver the messages via multiple routes to compensate for packet loss, and that events are often observed by multiple vehicles. As a result, vehicles can detect spoofed information by observing inconsistencies between the different received messages about the same event and it can be achieved at the cost of higher bandwidth usage and smaller information dissemination. Data redundancy is dynamically adjust in efficient dissemination protocols.

II.RELATED WORK

Earlier approaches to prevent spreading of malicious information secure vehicular communication design and infrastructure has been proposed in that first analyze threats and types of adversaries, identify security and privacy requirements, and present a spectrum of mechanisms to secure VC systems it can be quickly adopted and deployed but it does not included all the security challenges.Wischhof in 2005 proposed a inter vehicular communication based on segment oriented data abstraction and dissemination but it fails to provide prototype implementation of this SODAD approach. The next IEEE standard for wireless access in vehicular environments has been proposed in the year 2006 it introduces two types of access such as Road Side Unit (RSU) and Onboard unit(OBU) . the standard provided by this application is called Resource Manager(RM) The RM uses the concept of all of the communication being initiated from an entity known as a provider, which issues requests to an entity known as a user, which responds only to requests that it receives. In 2007 Liu and cheng proposed a system for insider attack detection in wireless sensor networks which meets all the requirements in spatial correlation in close proximity but does not specialized by exploring the degree of the correlations existent among different aspects of sensor networking behaviours. Raya and papadimitratos has proposed a data centric trust establishment in ephemeral ad hoc networks in 2008, it is inferred by Dempster-Shafer Theory. Several communication patterns were proposed by Buttyan and Holczer. A short paper was proposed in 2012 for dissemination redundancy to achieve data consistency in VANET's but It will not optimize path redundancy and bandwidth consumption at the same time.

III.OUR MODEL

In this paper, data-centric methods can be used to complement entry-centric method. To detect spoofed position data consistency checks are used that is the decisions are taken based on messages received from different sources .Three main types of data consistency mechanisms. Models can be used to compare claimed information against known models, such as the physical behavior of vehicles, local sensors can be used to verify

information received from vehicles in the direct vicinity and dissemination redundancy exploits the fact that messages are delivered via multiple routes to compensate for packet loss, the events are observed by multiple vehicles. Among these the redundancy-based approaches can be used even if the attacking vehicle is far beyond the reach of local sensors and compiles with physical models. Once inconsistencies are detected , we can use information from other sources to filter the incorrect information and possibly evict malicious nodes. Redundancy can be analyzed using graph-based metrics, such as redundant path(P), critical nodes(C) and distribution of information(D).These graph theory can be utilized to help understand the topological properties of a VANET, where the vehicles and their communication links can be modelled as vertices and edges in the graph, respectively. An efficiently computable metric for redundant paths based on the notion of the attackable message transfer. the attacker vehicle node can be eliminated by using a node-disjoint path, for example consider a graph G with vertices V and edges E we have to compute a helper graph with vertices V' and edges E' like G'(V',E'). Edmonds-Karp algorithm is used to calculate the number of node-disjoint paths consider as P. if P $\geq$ 2 then the number of critical nodes (C) is automatically zero. C indicates that how likely an attacker is successful. P and C measure suitability of protocol for redundancy based data consistency.

$$C = \begin{cases} 0, & P \geq 2 \\ |\{v \in V \backslash \{s,d\}; v \in C\}|, & otherwise \end{cases}$$

Distribution of information D as the fraction of all nodes that have received a particular message from the source. That is

$$D := |V(s,*)|/|V|$$

Safety-critical protocols will value high redundancy and a high number of paths over wide dissemination of potentially false information due to a higher number of critical nodes C.

Recently, a graph theoretical model called evolving graph has been proposed to help capture the dynamic behaviour of dynamic networks when mobility patterns are predictable. Architecture is shown below in Fig 1.

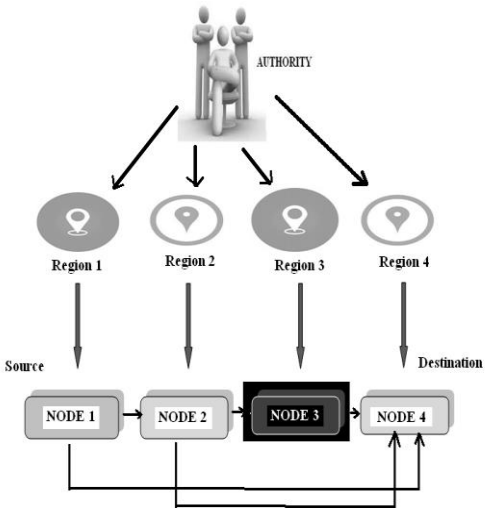

Fig 1 System Architecture

IV.OUR PROTOCOL

In our system, We will initialize all the vehicular nodes and authority to form a vehicular ad-hoc network. An authority will consists of several regions, Each regions in tern consists of number of vehicular nodes. based on the range and distance all the vehicular nodes are registered to their regions respectively in authority with its ID's, Then the authority will generate a valid key pairs using a key generation algorithm and distribute it to all the vehicular nodes in the network to make them ready for communication. Vehicular nodes in each region can communicate with other nodes in the same region or other region by establishing the routing protocols to the destination node to which the node want to communicate. Multiple paths can be formed to reach the destination node for data transmission, among that we have to find all the available path and redundant path to reach the destination node ,redundant paths are not considered for sending the data because it will not reach the destination node properly but we have to plot both available paths and redundant paths in the graph to analyse the metrics.

Find the possibility of all the critical nodes and plot them in the graph. Then we have to find the entire available path excluding the critical nodes which will reach the destination. From that available path we have to select the shortest path ,in order to send the data securely we have to encrypt the data using encryption algorithm . If the probability of critical node is more and if we can't reach destination without critical node we have to find the node disjoint path to reach the destination node so that a new path is formed, hence we

can exclude that critical node in our data dissemination protocol. In order to provide security to the forwarding message RSA algorithm is used to generate the valid key pairs and encrypt the transmitting message. the following image shows the Algorithm.

Key Generation

Select p, q	p and q both prime
Calculate n	$n = p \times q$
Select integer d	$\gcd(\phi(n), d) = 1; 1 < d < \phi(n)$
Calculate e	$e = d^{-1} \bmod \phi(n)$
Public Key	$KU = \{e, n\}$
Private Key	$KR = \{d, n\}$

Encryption

Plaintext: $M < n$

Ciphertext: $C = M^e \pmod n$

Decryption

Ciphertext: C

Plaintext: $M = C^d \pmod n$

The formation of vehicular ad-hoc network is shown below,R1,R2,R3and R4 are the four regions each region will have several number of vehicular nodes and a key is generated using RSA algorithm distributed to all the nodes in each region using authority node.

Fig 2 Implementation

V.CONCLUSION

In this paper, Insider attack detection scheme must be designed by enabling data consistency with dissemination-redundancy-based approaches are used to enable consistency checking in multiple data dissemination protocols such as advanced adaptive geocast and aggregation protocols to identify and eradicate the attacker nodes, in that a holistic protocols uses absolute cryptographic security measures that is RSA algorithm is used to enhance security measures by encrypting the important information communicated between vehicles and other infrastructure so the attacker node is not able to access the information, therefore Quality of service is achieved in packet delivery.

VI.REFERENCES

[1] Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl," Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols,"IEEE Trans.on vehicular technology..,May 4,2013.

[2] J. Petit, M. Feiri, and F. Kargl, "Spoofed data detection in VANETs using dynamic thresholds," in Proc. IEEE VNC, pp. 25–32,Nov. 2011.

[3] Mina Rahbari and Mohammad Ali Jabreil Jamali " Efficient detection of Sybil Attack based on cryptography in VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[4] Nedal Ababneh and Houda Labiod " Safety Message Dissemination in VANETs: Flooding or Trajectory-Based?"IEEE Trans ,2010.

[5] Stefan Dietzel_, Frank Kargl_, Geert Heijenk_, and Florian Schaub " On the Potential of Generic Modeling for VANET Data Aggregation Protocols"IEEE Trans on vehicular networking,Dec 2010.

[6] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs," IEEE Commun. Mag., vol. 46, no. 11, pp. 119–125,Nov. 2008.

[7] 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.

[8] 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, pp. 1238–1246, 2008.

[9] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in Proc. 26th IEEE INFOCOM, pp. 1937–1945,May 2007.

[10] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments- Security Services for Applications and Management Messages, IEEE Std. 1609.2-2006.

[11] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks," IEEE Trans. Intell. Transp. Syst., vol. 6, no. 1, pp. 90–101, Mar. 2005.

[12] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proc. 1st ACM Int. Workshop VANET, New York, pp. 29–37,2004.

[13] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: A survey," IEEE Wireless Commun., vol. 11, no. 6, pp. 6–28, Dec. 2004.

[14] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in Proc. 3rd ACMInt. Symp. Mobile Ad Hoc Netw. Comput., pp. 80–91,2002.

