ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Graph-Based Metrics Using Cryptography in VANET to Avoid Inside Attack

U.Vanitha, K.Vijayasamundeswari

Network Engineering, Arunai Engineering College, Tiruvannamalai, India

Department Of ECE, Arunai Engineering College, Tiruvannamalai, India.

ABSTRACT- VANET (vehicle Network) is emergent technologies that they deserve, recently, the attention of the industry and the academics institution .VANET is having many applications include safety applications, traffic efficiency enhancements, and infotainment service. vehicular network face more challenging task due to high speed and city environment characteristics. In this paper before using three protocols namely a geo-cast protocol ,baseline protocol And an aggregation protocol. a baseline represent the connectivity of node based on the chosen simulation, Advanced Adaptive Geo-cast (AAG) ,this protocol represent for Geo-cast protocol. An aggregation uses fixed road size segment ,its atomic observation are average. In this paper to increase the security for a vehicular communication introduce cryptography technique using one way hash shine algorithm

KEYWORDS: Cryptography, protocol analysis, vehicular Network(VANET),AAG**.**

I.INTRODUCTION

Future application that use of vehicular networking a wide range of use cases. We can difference main three groups of application:1)traffic efficiency 2)infotainment services applications, and 3) safety applications. safety applications main is to provide the driver with add in information that can prevent potential accident .Examples include its give to warning of hard breaking or a lane-change assistant. The main of traffic efficiency application is to best travel time beyond the possible of current navigation system .For instance, information about current average speed, which is dissemination to approaching vehicles, it can be help to best plan alternate some applications like video streaming or map updates while on the road.

Implements in vehicle-to-infrastructure communication (V2I) and vehicle-to-vehicle communication (V2V) have also increased.

The specific feature of VC are a two edged sword: a comfortable set of tools will be available but a formidable set of abuses and attacks may be present. Consider, for example, an attacker place large portions of the vehicular network with wrong information: a single compromised vehicle can transmit wrong hazard warning, which can then be taken up by all vehicles in both traffic streams. Particularly safety beacons which report the vehicle's positions and transactions, and infer private information about its driver and passengers[2].

Application dependence on vehicular communication range from very simple transmission of vehicle status data to more difficult large -scale traffic management including infrastructure integration. As a start to analyzing applications, this section gives an overview of envisioned application categories for vehicular networks. Although exact operation details are not yet standardized for most applications, and in spite the fact that such a collection can never be completely finished, the overview delivers basic mechanisms, components, and constraints involved in the system[3].

• Vehicles have a long life span, lasting several years in most cases. This makes it hard to change onboard systems in order to mitigate new risks to the vehicle safety.

• No technical expertise in vehicle electronics or VC security aspects is expected from a user who runs a vehicle. Hence, the vehicular security measures have to operate autonomously with no need for intervention or feedback from the user[4].

The vision for vehicular ad hoc networks (VANETs) includes the frequent exchange of data by vehicles (or nodes) to facilitate route planning, road safety and e-commerce applications. Network security is clearly important for each of these applications. The traditional approach to network security involves a key management solution that allows for data integrity and the authentication of network \insiders". Besides raising privacy concerns and being unwieldy for a VANET, we believe this approach solves the wrong problem. In a VANET, far simpler attacks than data modification exist, such as for example transmitting fraudulent data about road congestion or vehicle position, and such attacks can be quite damaging. Further, in large-scale VANETs there is no guarantee that previously honest nodes will not be corrupted in the future. Hence, security in a VANET relies upon the potentially more challenging problem of detecting and correcting malicious data[5].

II.RELATED WORK

Metrics:

We will now derive an efficiently computable metric for redundant paths based on the notion of an attackable message transfer. If a node exists that is part of all paths between *s* and *d*, then *G*(*s*,*d*) becomes disconnected after removing this node. Thus, the size of the graph's minimum vertex cut is 1. Applying Menger's theorems [6], We can use maximum flow algorithms to compute the number of node-disjoint paths efficiently. calculates the number of edge-disjoint paths for a source–destination pair in a weighted directed graph. We introduce a helper graph $G = (V, E)$ to obtain the number of node-disjoint paths as follows. Each node in V is split into two nodes v_i and v_i, and the two nodes are added to V. Thus

$$V = \{v1, v1, v2, v2, \ldots, vn, vn\}. \quad (1)$$

Now, an edge is added between all v_i and v_i pairs, and all incoming edges of G's nodes are added to v_i nodes, and all outgoing edges are connected with the v_i nodes, i.e.,

$$E = \{(v1, v1), \ldots, (vn, vn)\} \cup \{(vi, vj) : (vi, vj) \in E\}. \quad (2)$$

number of critical nodes (*C*) on the path between *s* and *d*. A node is critical if its removal would disconnect *G*(*s*,*d*).

$$P\ (a \in V \setminus \{s, d\} \text{ successful}) = C|V \setminus \{s, d\}| \quad (3)$$

Both *P* and *C* measure the suitability of a protocol for redundancy-based data consistency. However, such redundancy might come at the cost of higher bandwidth overhead. Therefore, we introduce distribution of information *D* as the fraction of all nodes that have received a particular message from the source. That is

$$D := |V(s, *)|/|V|. \quad (4)$$

Hence, *D* gives an intuition of a protocol's success rate in disseminating messages throughout a large area, which is a common goal for multihop communication protocols.

III.PROPOSED APPROACH

More research is necessary on protocols that explore the tradeoff between increased security due to redundancy on the one hand and dissemination efficiency on the other hand. Given our current results, we are able to detect inconsistencies in received information due to attackers. Moreover, we notice a high standard deviation due to the different network characteristics in all simulation settings. As a result, data consistency mechanisms that build on redundancy are bounded to be probabilistic rather than absolute in nature. A holistic protocol will use both absolute cryptographic security measures and probabilistic approaches together to ensure data consistency. In future, cryptographic techniques will be used to make this a complete protocol.

The goal is to analyze to what extent these protocols provide enough redundancy to detect attackers in different scenarios. We implemented representatives of the following protocol families.

Baseline: To have a baseline, we create a graph that represents the node connectivity based on the chosen simulation parameters. This graph resembles the result of a naïve flooding with perfect packet delivery even over multiple hops. The baseline gives an estimate of the maximum achievable redundancy in a network.

Geo-cast: We use an adaptive probabilistic gossiping protocol, namely, Advanced Adaptive Geo-cast (AAG) , as representative for the Geo-cast protocol family. In AAG, each node determines the message forwarding probability based on the current perceived node density according to two-hop neighborhood information. The protocol performance can be adjusted by configuring an average reception percentage, which states the percentage of nodes that should, on average, receive a message. In high node density scenarios, AAG uses a logistic function

to automatically reduce the forwarding probability further. A target region can be specified that determines the area for which an observation is relevant. For our simulations, we set the target region to the whole network, because we assume a traffic information application where all vehicles are interested in the speed of the other vehicles in the network.

Aggregation:We use a basic aggregation scheme similar to as representative for in-network aggregation protocols. The scheme uses fixed-size road segments, for which all atomic observations are averaged. For calculating our metrics, we assume that a message from the source reaches the destination if the destination receives an aggregate that the source message contributed to. All vehicles collect known aggregates in a world model and periodically disseminate a subset of the world model using one-hop linklayer broadcast. For dissemination, a fixed packet size is configured. In case the world model content exceeds the packet size, priority is given to information about the direct vicinity of the disseminating vehicle. Both segment size and dissemination packet size can be adjusted.

For these protocols and for each simulation setting, we calculate the redundant paths and critical nodes, between 100 randomly chosen source–destination pairs in different randomly selected node placements. All other vehicles, apart from participating in the forwarding process between the source and the destination, create and disseminate messages as well. These messages are regarded as background

One way hash chain algorithm:

One-way chains are an important cryptographic primitive in many security applications. As one-way chains are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature. Recent sensor network security protocols thus extensively use one-way chains to design protocols that scale down to resource-constrained sensors. A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way hash chain is the successive application of a cryptography hic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence. A hash chain is a successive application of a cryptographic hash function to a string.

IV.PERFORMENCE ANALYSIS

significantly if lower broadcast frequencies are used for AAG, which is due to the reduced number of packet collisions when using lower broadcast frequencies

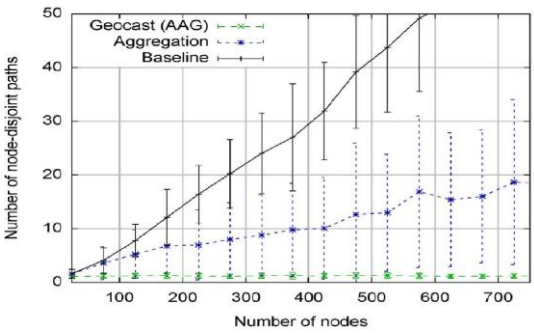

Fig:1 Node -disjoint paths

the aggregation protocol performs significantly worse than in the highway case. Even for high node densities, information exchange can be attacked in some cases. The reason for this is that the aggregation protocol needs to disseminate a much higher number of segments in the city scenario due to the larger road network.throughput getting increased

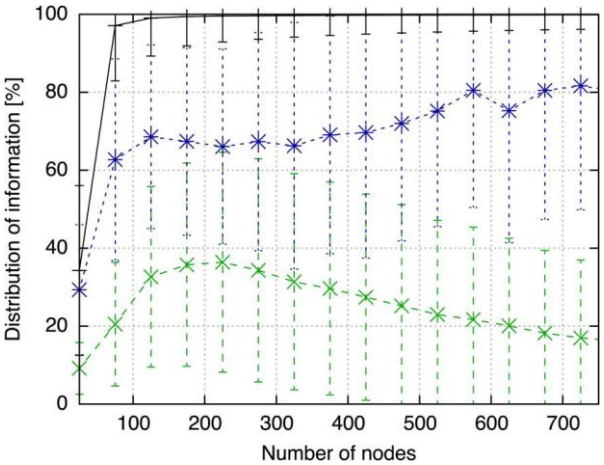

Fig:2 Distribution of information *D* for different node densities in a city

The higher number of road segments also reflects in the distribution of information .In contrast to the highway case, the aggregation protocol achieves a distribution of 60%–80% on average with a high standard deviation.

V.CONCLUSION

Data consistency is an important building block for secure vehicular communication systems. Focusing on entity-based solutions, such as message signing and certification using PKI, data consistency measures have been widely neglected by existing research. We have proposed a categorization of data consistency mechanisms into model-based, sensor-based, and dissemination-redundancy-based approaches and argue that redundant data forwarding paths are the most promising technique to enable consistency checks in multihop data dissemination protocols.A holistic protocol will use both absolute cryptographic security measures and probabilistic approaches together to ensure data consistency.

REFERENCES

[1] 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.

[2] 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.

[3] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Implementation, performance, and research challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 110–118, Nov. 2008.

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

[5] K. Menger, "Zur allgemeinen kurventheorie," *Fund. Math.*, vol. 10, no. 1, pp. 95–115, 1927.

[6] R. Bhandari, "Optimal physical diversity algorithms and survivable networks," in *Proc. 2nd IEEE Symp. Comput. Commun.*, 1997, pp. 433–441.

[7] F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof, "Executive summary—Inter-vehicular communication," in *Proc. Dagstuhl Semin. 10402—Inter-Veh. Commun.*, Wadern, Germany, Oct. 2010.

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

[9] M. Raya, P. Papadimitratos, V.D. Gligor, and J.-P. Hubaux, "On datacentric trust establishment in ephemeral ad hoc networks," in *Proc. 27th Conf. IEEE INFOCOM*, 2008, pp. 1238–1246.

[10] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Security Commun. Netw.*, vol. 3, no. 4, pp. 289–302, 2010.

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

[12] J. Petit and Z. Mammeri, "Dynamic consensus for secured vehicular ad hoc networks," in *Proc. IEEE 7th Int. Conf. WiMob*, Oct. 2011, pp. 1–8.

[13] 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.

[14] 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.

[15] B. Scheuermann, C. Lochert, J. Rybicki, and M. Mauve, "A fundamental scalability criterion for data aggregation in VANETs," in *Proc. 15th Annu. Int. Conf. MobiCom*, New York, 2009, pp. 285–296.

[16] *IEEE Standard For Wireless Access In Vehicular Environments (WAVE)- Multi-Channel Operation*, IEEE Std. 1609.4-2010, 2011 (Revision of IEEE Std. 1609.4-2006).

[17] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, no. 2, pp. 335–348, Apr. 1989.

[18] J. Wang and J. Silvester, "Maximum number of independent paths and radio connectivity," *IEEE Trans. Commun.*, vol. 41, no. 10, pp. 1482– 1494, Oct. 1993.