International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 15197-15206

http://www.ripublication.com

Efficient Scheme for Preventing Tunneling Attack in Vehicular Ad Hoc Networks

Komal Rana Kundan Munjal
Research Scholar Assistant Professor
Lovely Professional University Lovely Professional University
Punjab, India Punjab, India
ranakomal14@gmail.com kundan.16806@lpu.co.in

Abstract

VANET is vehicular adhoc network. Vehicles are transformed into the wireless nodes or routers of the network. Since, it is ad hoc network so there is mobility of host i.e. there is a change in topology in such a fashion so that interconnections between each host are capable of changing on continual basis. When there is a tunnel or jammed area the chances of the attack becomes maximum and since nodes are autonomous then the intruder nodes to attack or be the part of network are more because nodes exchange their positions based upon mutual trust . Thus any false node can send wrong information regarding routes and traffic inside the tunnel. This may cause various problems and road accidents. This paper depicts the solution that how to authenticate each node and how to establish a reliable network to prevent tunneling attack.

Keywords: ADHOC; MANETS; VANET; TUNNELING ATTACK; RFID.

Introduction

VANET uses adhoc communication for performing efficient data transmission .This intercommunication includes data from roadside and from other vehicles as shown in Fig 1. There are limitations of line -of –sight and ample processing delays. The router connectivity changes frequently and leads to the multi- hop communication. Routing protocols are there to facilitate communication within the nodes. These nodes

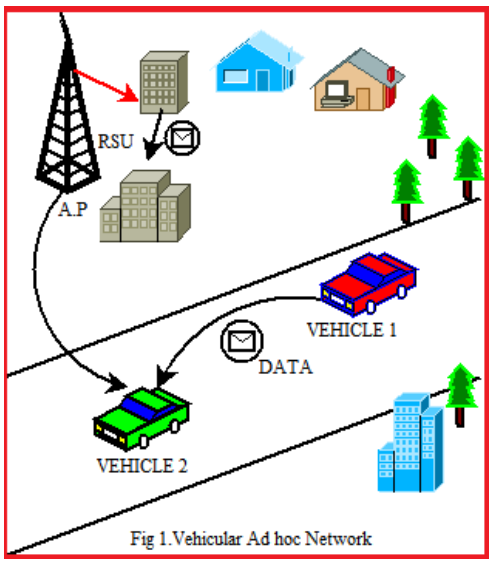

Fig 1.Vehicular Ad hoc Network

Arbitrary forms the topologies based upon their connectivity set up with each other. VANET works with a decentralized approach where nodes can communicate with each other on the basis of mutual trust and thus there is more possibility of attacks inside the network. When any host wants to communicate with another then these nodes must be within their range so that sender node can send data to destination and there can be the effective communication. During the communication there are intermediary nodes. Thus there are security issues in VANET as there may be the failure of data while communication of sender and receiver.

Tunneling Attack

Due to dynamic topology an attacker exploits information when a vehicle enters into a tunnel. Thus attacker now can steal significant information within the network. An attacker connects two distinct parts of the network using an extra communication channel as a tunnel.

This may be actual physical tunnel or jammed area. In Fig2 C1 and C2 are two units of communicational channel entering inside the tunnel; AP is access provider for both the communication channel. This tunnel is jammed area that is created by the intruder. Users assumes it as the same communication channel thus continues exchanging the data but in actual; it was a tunnel created by any false entity.

In tunneling attack there is:

A. Attack on authentication:

Since there is random change in the topology of the network within the tunnel any false host can readily enter into the tunnel as there is no appropriate method of authentication

of nodes. Thus attacker can cause message alteration message suppression, traffic jamming by creating replica copies of same host into the tunnel.

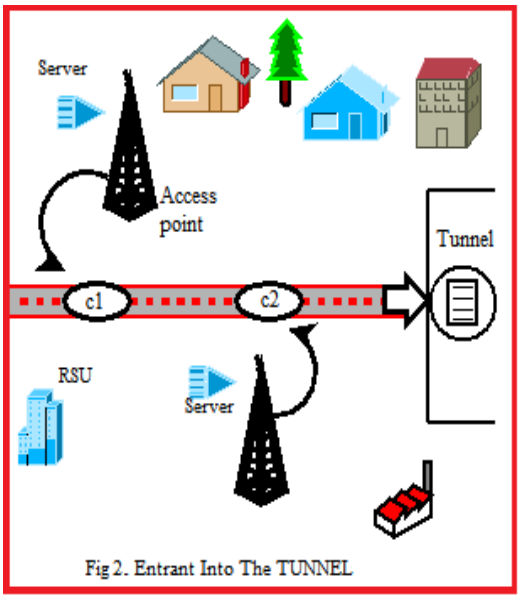

Fig 2. Entrant Into The TUNNEL

Hence there should be appropriate mechanism for authentication.

B. Attack on availability:

There is Denial of Service attack by the vehicle inside the tunnel, communication channel must be available at all the time otherwise there is possibility of denial of service attack. This obstruction may cause entire network failure in delivering packets and thus data is not available all the time for other nodes in the network.

C. Attack on trust:

No user wants to reveal the secret information about its time, locality, speed and data, transmitted into the mesh. All sensitive data must be taken care carefully. Lack of authentication, less availability of data thus there is less trust among the nodes of the tunnel.

D. Attack on Driver Confidentiality

Since in vehicular adhoc network there is no exchange of the secure information within the network. But data exchange should take place between the authenticated users only. So that only trusted users are within the tunnel and no loss to data confidentiality.

E. Attack on privacy:

[2] Driver privacy is an important issue in vehicular adhoc network. They don't want their private information to be accessed by another. Driver's identity should not be steal by another attacker in the node because it may contain the speed, locality, time and data that to be transmitted into the network Thus when a node/vehicle enters into a tunnel then In order to setup a connection within a network at least three satellites are required but it's not practicable inside a tunnel to have a range of three satellites. Moreover GPS signals can't be used without effective network inside the tunnel. So we can have unique identifiers: RFID number. Radio Frequency Identification Number, used to electrically recognize the presence of any object. As shown in Fig 3 road side units have RFID tags for authentication. These numbers are provided to each and every host /vehicle which is entrant into the

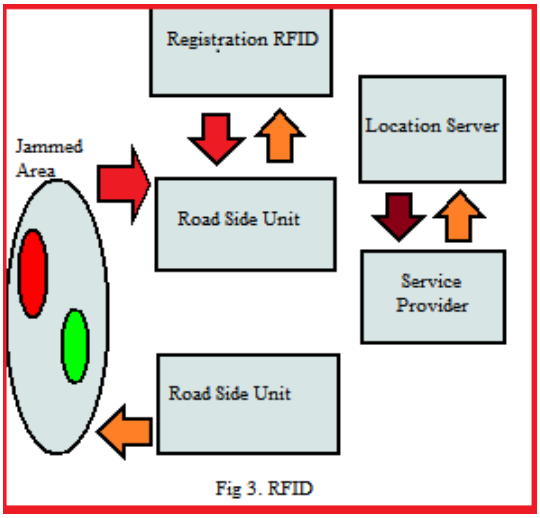

Fig 3. RFID

tunnel by certificate authorities. RFID are decided by these authorities and are saved into the databases for the entries of vehicles into the tunnel. Thus we have all the records of the nodes those are within the tunnel.

The RFID number represents the following field entries of vehicles into the tunnel:

A. Reserved Memory:

This memory usually stores the access kill password and password and is very infrequently used and is used to permanently disable the tags whereas accessibility of password is set to lock and unlock the tag's read /write capabilities. But it can store Only 2 tag information and it's applicable only in case of sensitive data. It's writable if you want to specify fixed password.

B. Tid Memory:
This tag is basically provided by the manufacturer it's generally IC number. This memory portion is fixed and can't be changed.
C. EPC Memory:
This memory stores Electronic Product Code .its first writable memory bank with 96 bits of memory.

D. User Memory:
If there is need of more memory then EPC the ICs have user memory which can store more information. But there are no standard defined for memory/bits that are writable on each tag. This is second writable memory tag. Memory tag is prolonging up to 4K to 8K. Thus we can store all the information concerning any vehicular host into our databases and there will be less probability of entrant any false node into tunnel.

1. Mechanism of RFID technology:
RFID tags are values assigned to the variegated entities/nodes entrant in the tunnel. Fig- 4 shows the working of RFID Tags. These tags are made up of integrated circuits antenna. There are readable and writable the antennas thus receive and transmit electromagnetic waves. There are RFID readers that recognize these values and stores into the databases. These Readers transform the Electromagnetic signals received from antennas into signals. The values stored by RFID reader contains various fields as explained in above section. In order to check whether the entity is valid its value is checked into the database and hence can determine whether the node is fake or not. This was all about the case that only the certified authorities are entering into the tunnel even in the case if the nodes within the network become selfish and may cause certain problem within

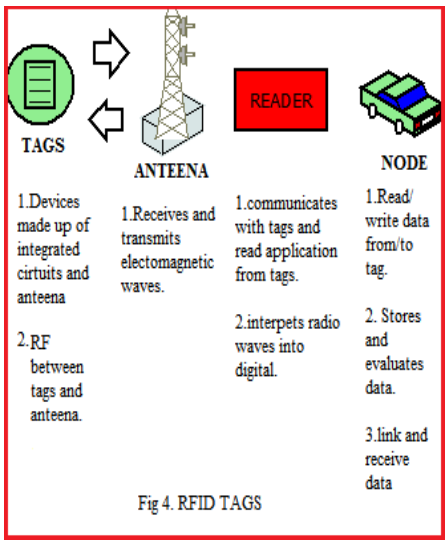

Fig 4. RFID TAGS

the network then we have watchdog mechanism to control this effect. Here is simple idea about these techniques:

A. Core (Within The Network):

After RFID in the network there should be a mechanism so that within the network if there is some self-centered node we can discover them there will be a reputation table that will be containing:

a) All routes.
b) Entries of self-centered node if any.

Reputation table is basically a data structure that is stored in each entity .Each row in the table comprise of:

- Behavior of each node.
- Identifier attached with each node.
- List of secondary reputation path with another identity.

Thus we can have a watch on the node if the node is not forwarding packets to another nodes in the network then it's a self- centered node. From reputation table we can easily reexamine by the identifier and from list that which node is self-centered and thus selfish node can be easily removed from the network.

Thus now we have mechanisms before entering the tunnel, inside the tunnel discovery of false node then when any vehicle will come out of the tunnel then in that case also there should be certain mechanisms so that we can have secure network just outside the tunnel. There can be various mechanisms related to authentication of nodes so that authenticated nodes can enter into the tunnel.

B. Token Based Approach (Outside The Tunnel):

As the Fig 5 shows the entrant node inside the tunnel, a token is required to participate in the network include the period that node want to be in the network. All its regional neighbors collectively supervise it and reports it .If the token of the node get expired then new values are also assigned to them since the nodes that are coming outside from the

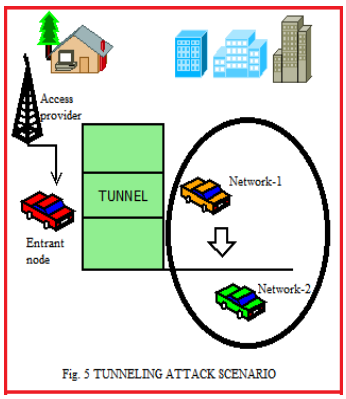

Fig. 5 TUNNELING ATTACK SCENARIO

Tunnel, are the main part of our network and these nodes will serve as the neighbors to the nodes that were on different network.

Thus basically a mapping of two networks is required here. Thus the token is renewed and the entries of all the nodes is recorded in a table although it's dynamic table but still there will be a monitoring for all the nodes in order to detect a false node.

There may be the case that we can consider that instead of using the token based approach we can also go for the network mapping i.e. we have assured network because of the technologies incline while entering and also inside the tunnel and we can also detect the false node inside the tunnel. Therefore now we can simply use the mapping or the shifting of our network that is within the tunnel to other network while exiting the tunnel as shown in Fig 6.

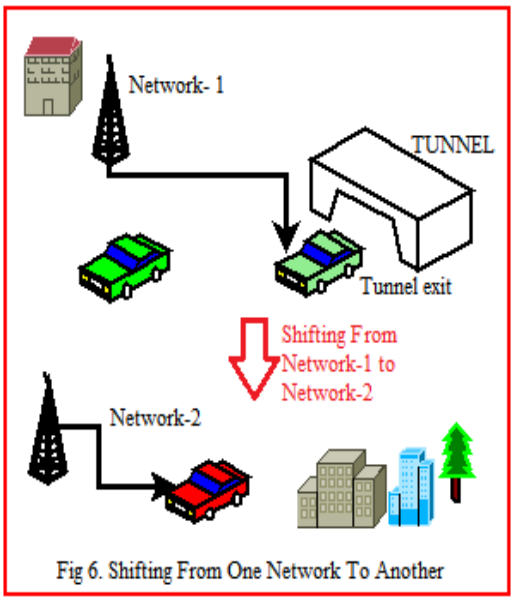

Fig 6. Shifting From One Network To Another

Critical Analysis

It is not always the case that if there is delay in the packets then we will consider it as a tunnel but sometimes there may be the case that there is a false node in the system that may also cause delay in the transfer of data between the communicating nodes.

By the help of communicating group nodes we can track the location of false node from the node to which it was communicating. After detecting the location of node we can detect whether the node was actually not transferring the data was false node or there was a problem in the network. RFID can sense the network and thus we can detect the status of the nodes whether there was a tunnel in reality or it was only because of the false node in the network.

In order to have more and more security from intruder into the network there should be the usage of RFID tags into the network within the tunnel it will help us in sustain our databases and records of all the nodes .So that only the authenticate nodes can enroll into the network. We can also have a check on false node so that the availability of the nodes can be easily accused and we can preclude our network from false node. Since now network is secure then no attack on the confidentiality. As now we have a confidential network then there will be no attack on security of the network. These all are preventive measures for the attack while intruder is entrant or inside the tunnel and when all the traffic is exiting from the tunnel then we can deviate all the nodes onto a different network as all the nodes even a selfish node can be easily traced thus we have a better network security and no attack vulnerabilities while entering, inside the tunnel and after exiting the tunnel. Thus we have a secured network.

Future Work

Tunneling attack can be prevented as the methods suggested in the previous sections. But in case if the false node is not detected within the network and then we cannot prevent the attack inside the tunnel. This will cause problem for the several security issues also if we are applying the method of mapping of network that was within the tunnel to the to the other then the nodes that are also outside the tunnel may face problems or issues regarding the network although token based approach will not lead to the problems .In case a small range network we can use the network mapping approach.

Acknowledgment

Foremost, I would like to express my sincere gratitude to my guide Professor Kundan Munjal for continuous provision of my M.Tech study and research, for his patience, motivation, enthusiasm, and immense knowledge. His supervision helped me in writing of review paper and continuing my thesis work.

I want to thank higher authorities of Lovely Professional University for providing me the opportunity of writing a paper.

Last but not the least; I would thank my family for supporting me spiritually throughout my life.

References

[1] Mohammed Saeed Al-kahtani “Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)” Computer Engineering Dept., Salman bin Abdulaziz University, Saudi Arabia 2012.

[2] Farzad Sabahi, “The Security of Vehicular Adhoc Networks” Faculty of Computer Engineering .AzadUniversity Third International Conference on Computational Intelligence, Communication Systems and Networks, 2011.

[3] J.T. Isaac S. Zeadally J.S. Ca´mara , “Security attacks and solutions for vehicular ad hoc networks” IET Communications 2009.

[4] R. Akbani, T. Korkmaz, G.v.S Raju," HEAP: A packet authentication scheme for mobile ad hoc networks", ad hoc network, v.6 n.7, p.1134- 1150, 2008.

[5] PARNO B., PERRIG A.: „Challenges in securing vehicular networks . Fourth Workshop on Hot Topics in Networks (Hot Nets-IV), 2005 [6] FLORIAN D., LARS F., PRZEMYSLAW M.: „VARS: a vehicle ad hoc network reputation system. Int. Conf. on a World of Wireless, Mobile and Multimedia Networks” (WOWMOM 2005), 2005, pp. 454 456

[6] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda “Over-view of security issues in Vehicular Ad-hoc Networks”, 2007.

[7] Swapnil G. Deshpande “Classification of Security attack in Vehicular Adhoc network: A survey”, in the department of Arts, Commerce, Science College, Kiran Nagar, Amravati, Maharashtra, India.2011

[8] Mohammad Fanaei', Mehdi Berenj koub , Ali Fanian “Resistant TIK-Based endairA Against the Tunneling Attack” Department of Electrical and Computer Engineering, Isfahan University of Technology (IUT), Isfahan, Iran2008.

[9] Q.Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, “Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[10] A.Perrig and D. Song “Random key pre- distribution schemes for sensor networks”. In IEEE Symposium on Security and Privacy, pages 197–213, Berkeley, California, May 11-14 2003.

[11] M.Raya and J.P. Hubaux, 2007,” Securing vehicular ad hoc networks”. Journal of Computer Security, 15(1), 39–68.

[12] S. Capkun, L Buttyan and J.-P. Hubaux, “SECTOR: Secure Tracking of Node Encounters in Multichip Wireless Networks,” Proc. ACM Wksp. Sec. of Ad Hoc and Sensor Networks, Fairfax, VA, Oct. 2003.

[13] “IEEE trial-use standard for wireless access in vehicular environments (wave)- security services for applications and management messages,”IEEE, New York, NY, IEEE Std 1609.2, Jul. 2006..

[14] Hou Wang, Chunxiao Chigan, “Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs” Communications, 2007. ICC ’07. IEEE International Conference on Digital Object Identifier: 10.1109/ICC.2007.652 Publication Year: 2007, Page(s): 3959-3964

[15] R. Parker, S. Valaee: “Vehicle localization in Vehicular Networks” .in: Vehicular Technology Conference, 2006. VTC 2006 Fall 2006 IEEE 64th, 2006, pp. 1–5.

[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *MOBICOM*, 2000, pp. 255 –265.

[17] L. Eschenauer and V. D. Gligor "A key- Management scheme for distributed sensor networks".In Proceedings of the 9th ACM conference on Computer and communications security, November 2002.

[18] Jun-ZhaoSun, Machine Vision & Media Process Unit, Oulu Univ, Finland: "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", pp. 316 -321 vol.3, 2001

[19] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, Apr. 2003, pp. 270–280.