AN EFFICIENT MESSAGE AUTHENTICATION SCHEME BASED ON EDGE COMPUTING FOR VEHICULAR AD HOC NETWORKS

MALLA GANA SANKAR [#1], A.DURGA DEVI [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

With the progress in wireless communication technology and the increasing number of vehicles, vehicular ad hoc networks (VANETs) have become essential for improving road conditions and enhancing driving experience. The core of the VANETs is the communication between different vehicles, and the security of the communication is based on message authentication. In our scheme, the roadside unit can efficiently authenticate messages from nearby vehicles and broadcast the authentication results to the vehicles within its communication range, thereby reducing redundant authentication and enhancing the efficiency of the entire system. The security analysis results show that the proposed scheme satisfies the security requirements of the VANETs.

1. INTRODUCTION

WITH the development of the automobile industry and the improvement in the economy, vehicles have become increasingly important. However, the increase in the number of vehicles has led to rising traffic congestion and frequent traffic accidents. Therefore, there is a need to improve driving experience and enhance driver safety. This has led to the research of vehicular ad hoc networks (VANETs) with the aim of enhancing driver safety through inter-vehicle communications (V2V) and communications with public infrastructure (V2I) [2]. The typical structure of VANETs comprises three parts: a trusted authority (TA), a roadside unit (RSU), and an on-board unit (OBU). The TA, which acts as the trusted management center, is responsible for the registration and issuing of secret key material.The RSU, installed along the roads, serves as a bridge between the vehicles and the TA.

The OBU equipped on each vehicle is in charge of the V2V and V2I communications [3], [4]. As V2V and V2I communications are wireless, malicious attackers can modify the message sent from a vehicle, and even disguise themselves as vehicles if there is no adequate security scheme for the VANETs. Therefore, in VANETs, the message recipient should check the integrity and reliability of the received message. Only if the message is credible, the information contained in the message can be trusted. In

recent years, privacy has become a topic of concern with regard to VANETs. No driver would like to have information, such as driving route or identity, be leaked. Thus, the communication protocol in the VANETs should satisfy anonymity, implying that a vehicle should communicate with all entities via pseudo identity instead of a real one [5]. However, a completely anonymous scheme should be avoided because of the following reasons. Although we cannot avoid the appearance of malicious vehicles that could send forged messages or attempt to modify the valid messages, we can trace malicious vehicles and determine their real identities. In the VANETs, we consider schemes with such capacity to satisfy the conditional privacy- preserving (CPP) characteristic [6], [7].

1.2 PROBLEM STATEMENT

In the existing system we there is no proper mechanism which can schedule the authentication scheme for data transfer.Hence all the data which is send from sender to receiver will be passed through intermediate router and if the router is not having a strict facility to choose best path,then data will be lost.

The existing networks didn't concentrated on the property of path configuration. In the existing networks if there was any node revocation occurred in the network ,entire architecture need to be changed and hence it is a delay process. If the node failed in the transfer the router will stop the data transmission in the middle. There was a huge delay performance in the existing routing technique.

In our proposed scheme, the roadside unit can efficiently authenticate messages from nearby vehicles and broadcast the authentication results to the vehicles within its communication range, thereby reducing redundant authentication and enhancing the efficiency of the entire system. The security analysis results show that the proposed scheme satisfies the security requirements of the VANETs.

2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

RELATED WORK

1) MULTICAST CAPACITY OF WIRELESS AD HOC NETWORKS

PUBLICATION: X.-Y. Li, IEEE/ACM Trans. Netw., vol. 17, no. 3, pp. 950-961, June 2009.

We study the multicast capacity of large-scale random extended multihop wireless networks, where a number of wireless nodes are randomly located in a square region with side length a = √n, by use of Poisson distribution with density 1. All nodes transmit at a constant power P , and the power decays with attenuation exponent α > 2. The data rate of a transmission is determined by the SINR as Blog(1+ SINR), where B is the bandwidth. There are ns randomly and independently chosen multicast sessions. Each multicast session has k randomly chosen terminals. We show that when k ≤ θ 1 [(n)/((logn) 2α+ 6)] and ns ≥ θ 2 n 1/2+β , the capacity that each multicast session can achieve, with high probability, is at leastc 8 [(√n)/(ns√k)], where θ 1 , θ 2

, and c 8 are some special constants and β > 0 is any positive real number. We also show that for k = O([(n)/(log 2 n)]) , the per-flow multicast capacity under Gaussian channel is at most O([(√n)/(ns √k)]) when we have at least ns = Ω(logn) random multicast flows. Our result generalizes the unicast capacity for random networks using percolation theory.

2) MULTICAST CAPACITY OF WIRELESS AD HOC NETWORKS UNDER GAUSSIAN CHANNEL MODEL

PUBLICATION: X.-Y. Li, Y. Liu, S. Li, and S. Tang, IEEE/ACM Trans. Netw., vol. 18, no. 4, pp. 1145-1157, Aug. 2010.

We study the multicast capacity of large-scale random extended multihop wireless networks, where a number of wireless nodes are randomly located in a square region with side length a = √n, by use of Poisson distribution with density 1. All nodes transmit at a constant power P , and the power decays with attenuation exponent α > 2. The data rate of a transmission is determined by the SINR as Blog(1+ SINR), where B is the bandwidth. There are ns randomly and independently chosen multicast sessions. Each multicast session has k randomly chosen terminals. We show that when k ≤ θ 1 [(n)/((logn) 2α+ 6)] and ns ≥ θ 2 n 1/2+β , the capacity that each multicast session can achieve, with high probability, is at leastc 8 [(√n)/(ns√k)], where θ 1 , θ 2 , and c 8 are some special constants and β > 0 is any positive real number. We also show that for k = O([(n)/(log 2 n)]) , the per-flow multicast capacity under Gaussian channel is at most O([(√n)/(ns √k)]) when we have at least ns = Ω(logn) random multicast flows. Our result generalizes the unicast capacity for random networks using percolation theory.

3) MULTICAST CAPACITY FOR HYBRID WIRELESS NETWORKS

PUBLICATION: X. Mao, X.-Y. Li, and S. Tang, in Proc. ACM MobiHoc, Hong Kong, 2008, pp. 189-198.

We study the multicast capacity for hybrid wireless networks consisting of ordinary wireless nodes and base stations under Gaussian channel model, which generalizes both the unicast capacity and broadcast capacity for hybrid wireless networks. We simply consider the hybrid extended network, where the ordinary wireless nodes are placed in the square region A(n) with side-length radicn according to a Poisson point process with unit intensity. In addition, m additional base stations (BSs) serving as the relay gateway are placed regularly in the region A(n) and they are connected by a high-bandwidth wired network. Three broad categories of multicast strategies are proposed in this paper. According to the different scenarios in terms of m, n and n d , we select the optimal scheme from the three categories of strategies, and derive the achievable multicast throughput based on the optimal decision.

4) CLOSING THE GAP OF MULTICAST CAPACITY FOR HYBRID WIRELESS NETWORKS

[4] S. Tang, X. Mao, T. Jung, J. Han, X.-Y. Li, B. Xu, and C. Ma, in Proc. ACM MobiHoc, Hilton Head, Italy, 2012, pp. 135-144.

We study the multicast capacity of a random hybrid wireless network consisting of wireless terminals and base stations. Assume that n wireless terminals (nodes) are randomly deployed in a square region and all nodes have the uniform transmission range r and uniform interference range R = Θ(r); each wireless node can transmit/receive at Wa- bps. In

addition, there are m base stations (neither source nodes nor receiver nodes) that are placed uniformly in this square region; each base station can communicate with adjacent base stations directly with a data rate WB-bps and the transmission rate between a base station and a wireless node is Wc-bps. Assume that there is a set of ns randomly selected nodes that will serve as the source nodes of ns multicast flows (each flow has randomly selected k−1 receivers). We found that the multicast capacity for hybrid networks has three regimes and for each of regimes, we derive the matching asymptotic upper and lower bounds of multicast capacity. Index Terms—Hybrid networks, capacity, multicast, broadcast.

3. EXISTING STATEMENT

In the existing system we there is no proper mechanism which can schedule the authentication scheme for data transfer. Hence all the data which is send from sender to receiver will be passed through intermediate router and if the router is not having a strict facility to choose best path,then data will be lost.

LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They are as follows: The existing system didn't concentrated on the property of path configuration. In the existing system if there was any node revocation occurred in the network ,entire architecture need to be changed and hence it is a delay process. If the node failed in the transfer the router will stop the data transmission in the middle. There was a huge delay performance in the existing routing technique.

4. PROPOSED SYSTEM

In our scheme, the roadside unit can efficiently authenticate messages from nearby vehicles and broadcast the authentication results to the vehicles within its communication range, thereby reducing redundant authentication and enhancing the efficiency of the entire system. The security analysis results show that the proposed scheme satisfies the security requirements of the VANETs.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows: The current system mainly concentrated on the property of path configuration. In the current system if there was any node revocation occurred in the network , there is no need to change the entire architecture. Less delay for transfer Huge efficiency and accurate. If the node failed in the transfer then our router will generate alternate path

5. SOFTWARE MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed protocol. The front end of the application takes Java Swings and AWT and as a Back-End Data base we took My-SQL Server. The application is divided into 5 modules. They are as follows:

1) Sender Module

2) Router Module

3) TA Module

4) Receiver Module

5) Node Failure Module

Now let us discuss about each and every module in detail as follows:

5.1 Sender Module

In this module, the sender will request MAC address of particular vehicle to Trusted Authority, after requesting, the trusted authority will give response to sender. After getting a Mac address the sender will brose the file and upload to the vehicular router, the vehicular router will send to the particular receiver (A, B, C, D, E), after receiving successful sender will get a response. If sender will enter a fake Mac address, then he will be considered as an attacker.

5.2 Router Module

In this module, we can see the all vehicle details and allocate MAC address. In a vehicular router, the sender will allocate MAC address for each & every vehicle node, and before allocating Mac address, he will enter validity of particular vehicle such as valid from, valid to, IP address and submit, then he will get a response vehicle name & MAC address assigned to particular vehicle. If we clicks on view vehicular details, it will display all details with their tags such as vehicle name, token no, valid from, valid to, IP address and attacker status. The vehicular router will receive the file from service provider and then send to the particular receiver.

5.3 TA Module

The TA will receive the allocated Mac address from the vehicular router, whenever the sender will request a Mac address, then the trusted authority will distribute Mac address of particular vehicle. After getting a Mac address the sender will browse the file and send to the particular receiver (A, B, C, D, and E).

5.4 Receiver Module

In this module, there are n-number of receivers are present (A, B, C, D, E and F). The receiver can receive the data file from the sender via vehicular router. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the router only.

5.5Attacker Module

Attacker is one who is injecting the fake Mac address and changes the IP address of the corresponding vehicle nodes. The sender will enter a fake Mac address, then router will considered as message integrity attacker. If the attacker changes IP address of particular node, then he will be considered as privacy identity attacker. The attacker details will store in attacker list with their tags such as attacker type, attacker name, attacked node, time & date.

6. OUTPUT RESULTS

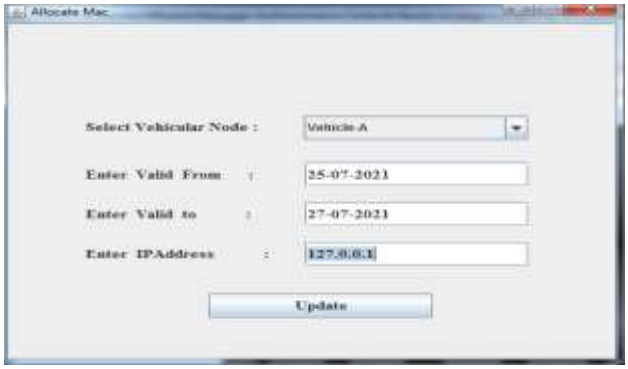
RECEIVER D WINDOW

Receiver E Window

TA WILL GRANT MAC KEY

SOURCE NODE CHOOSE A TEST FILE

UPDATE MAC ADDRESS



Represents the Text File which is encrypted and send to router

7. CONCLUSION

We for the first time designed a secure application which can able to send data under a dedicated VANETs which contains several MAC address and based on that we are going to transfer the data from sender to receiver under a dedicated path.

8. REFERENCES

[1] X.-Y. Li, ‘‘Multicast Capacity of Wireless Ad Hoc Networks,’’IEEE/ACM Trans. Netw., vol. 17, no. 3, pp. 950-961, June 2009.

[2] X.-Y. Li, Y. Liu, S. Li, and S. Tang, ‘‘Multicast Capacity of Wireless Ad Hoc Networks under Gaussian Channel Model,’’ IEEE/ACM Trans. Netw., vol. 18, no. 4, pp. 1145-1157, Aug. 2010.

[3] X. Mao, X.-Y. Li, and S. Tang, ‘‘Multicast Capacity for Hybrid Wireless Networks,’’ in Proc. ACM MobiHoc, Hong Kong, 2008, pp. 189-198.

[4] S. Tang, X. Mao, T. Jung, J. Han, X.-Y. Li, B. Xu, and C. Ma,‘‘Closing the Gap of Multicast Capacity for Hybrid Wireless Networks,’’ in Proc. ACM MobiHoc, Hilton Head, Italy, 2012,
pp. 135-144.

[5] W. Huang, X. Wang, and Q. Zhang, ‘‘Capacity Scaling in Mobile Wireless Ad Hoc Network with Infrastructure Support,’’ in Proc. IEEE ICDCS, Genoa, Italy, 2010, pp. 848-857.

[6] Y. Guo, F. Hong, Z. Jin, Y. He, Y. Feng, and Y. Liu,‘‘Perpendicular Intersection: Locating Wireless Sensors with Mobile Beacon,’’ IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3501-
3509, Sept. 2010.

[7] C. Wang, X.-Y. Li, S. Tang, C. Jiang, and Y. Liu, ‘‘Capacity and Delay in Mobile Ad Hoc Networks under Gaussian Channel Model,’’ SIGMOBILEMobile Comput. Commun. Rev., vol. 14, no. 3, pp. 22-24, July 2010.

[8] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Advances in Cryptology*. Berlin, Germany: Springer, May 2005, pp. 457–473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Oct. 2006, pp. 89–98.

[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, “Efficient attribute-based encryption from R-LWE,” *Chin. J. Electron.*, vol. 23, no. 4, pp. 778–782, Oct. 2014.

[11] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.

[12] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, Oct. 2007, pp. 456–465.

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated ciphertext-policy attribute-based encryption and its application,” in *Proc. 10th Int. Workshop Inf. Secur. Appl.*, Aug. 2009, pp. 309–323.

[14] X. Xie, H. Ma, J. Li, and X. Chen, “An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing,” *J. Universal Comput. Sci.*, vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[15] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, “CP-ABE with constant-size keys for lightweight devices,” *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.