Volume 6, Issue 8, August 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Trust Based Scenario using AES Encryption in VANET

Sudha Dwivedi, Rajni Dubey, Nirupma Tiwari
Department of CSE/IT, SRCEM College, Banmore, Gwalior,
Madhya Pradesh, India

Abstract— Security is the main concern of any other network because of if attacks apply in networks than users suffer and quality of service is down when we talk about VANET which is highly moveable or infrastructure of VANET change frequently in this network security is main concern because if its flexible and secure passengers feel convenient to travel. Trust is the most important area, to build trust between vehicles we apply behavior based technique for passive attack we use AES encryption.

Keywords— VANET, AES, V2V, V2I

I. INTRODUCTION

VANET is part of MANET, it means that all node may move freely in stay connected and network coverage, all node may communicate using further nodes in multi hop or single hop and any node could be Vehicle, RSU. Usually, this can connect to vehicles within variety of 100 to 900 meters if using 802.11p. It is needed to realize that the ITS aims to improve road security and provides a comfortable travel experience to driver and passengers [1] [2]. There have been various research initiatives for example CVIS, COOPERS, PReVENT, SAFESPOT, ASV and WAVE carried out across Europe, Japan and US to make ITS into a reality. Non Security applications permit passengers to access many services like interactive communication, internet access, payment services, online games and information updates whilst vehicles are on move. The notable dissimilarity between safety and non-safety application is that safety applications are capable of sending and processing messages in actual time [3]. The passengers and driver may access both kinds of services from the nearby infrastructure seamlessly using wireless access technologies [4]. VANET and MANET have lots of similarities for example dynamic topology, multi-hop data transmission, distributed architecture and Omnidirectional broadcast. Mobile nodes are able to relay or route data to endpoint by itself in both networks. Nevertheless, there are some notable variance between MANET and VANET. Since the vehicles are moved along road, the mobility of nodes in VANET is predictable unlike MANET [5]. Moreover, there is no limitation of processing and storage ability also battery power of nodes in VANET. Because of fast movement of nodes in VANET formed wireless network topology is highly dynamic. Additionally, network density in VANET varies over time and location significantly [6]. Typically, VANET involves of four major components namely: Vehicles, Devices/Sensor for example GPS enabled devices, Road-side Info-Stations and Traffic Management Centre (TMC) [7] [8]. All these components communicate using wireless communication standards/protocols that will determine the many aspects of communication such as data transmission range and rate, latency and security. Possibly, message delivery is deliberated as key challenge because of fast topology change, frequent signal disruptions, and contact opportunities of VANET [9] [10].

Fig 1. VANET

II. TRUST IN VANETS

Trust Models in VANET there are different main trust models: Entity-oriented believe models, information-oriented believe models, mixed trust models. Entity-oriented believe models center of helpfulness on trustworthiness of peers. It's divided into sociological trust model proposed in and multifaceted believe administration mannequin proposed. The sociological trust mannequin is established on the principle of reliance and self-belief tagging. Situational trust is

determined by the node's condition, while dispositional belief is the peer's possess beliefs. System believe rest on the system security level, however, belief development system is the evaluation of data founded on the prior factors.

Role based believe will depend on the function a node plays in society, e.g. Police car. Experience-based trust is built between nodes after several interactions. Data-oriented believe items depend on evaluating trustworthiness of transmitted information. In such models, no long-term believe relationships between nodes are shaped. Data-centric believe institution evaluates trustworthiness of reported data rather than the believe of the entities. Mixed trust model make use of node's trust to assess trustworthiness of information, where node's trust is maintained by time. Opinion piggybacking is when all nodes appends its opinion to the message earlier than forwarding it. Believe-based message propagation and analysis framework in vehicular advert-hoc networks is when nodes share information regarding road condition or safety messages and others provide their opinions. Preauthenticated anchor nodes, are previously predefined nodes and are considered as dependable. Characteristics of believe items in vehicular atmospheres should be:

1. Decentralized
2. Copes with scarcity of information
3. Location and time specific
4. Trust is a task
5. Scalable

A Central Authority cannot decide this because this might be far away (say a government security agency). An interesting question will be to model the profits and prices with the changing network topology[11].

Umar et al. [12] examine challenge of planning intelligent agents to enable distribution of information between vehicles in MANET. Their concentration was on developing framework that models trustworthiness of agents of further vehicles so as to receive most effective reports. The framework is up to restrict amount of reports that are received. The writers developed many-facet trust modeling framework that incorporates rolebased trust, trust experience-based and trust majority based. Authors included lgorithm to integrate these many dimensions of trust, along with experimentation to validate benefits of their method. The authors clarified how their approach was able to meet various critical challenges for trust modeling in VANETs. As a final result they presented methodology to allow V2V communication via intelligent agents. The authors propose that, that derive a rather comprehensive and complete view of trust for agents in VANET environments, this is needed to integrate security solutions using trust management. The core of model is divided in 2 parts. The authors emphasized significance of dissimilar facets that were included. First one is composed of experience-based, priority based trusts and role-based. These trusts maintain trustworthiness of agents in order for trusted agents to be chosen for their feedback. The first 2 trusts are joined into priority-based trust,that may be accustomed select proper advisors. Agents may put more trust in certain agents as compared to others The experience-based trust represents a component of trust that is founded on direct interactions among agents. The 2nd part of model is composed of the majority opinion. It part aggregates feedback from selected advisors. Based on it model, when agent in VANET receives reports from extra agents about. event, eg., traffic or collision ahead, it may essential to verify if e information received is reliable. To do so, agent asks other trusted agents about the received information. For this purpose, All agent in system keeps track of list of other agents. The role-based method is founded on following 4 dissimilar roles listed in decreasing significance: authority, expert, ordinary. The problem using this method is to take on that nodes may maintain list of untrusted and trusted agents in addition to that this is likely to request "advices" about message. The ephemeral nature of VANET leads to very short lived relationship between nodes, for which isn't possible to build an effective list of trusted nodes to ask for advices. Moreover, because of speed all node is moving in network, when an advice arrives this can be too late for node to consider it.

III. LITERATURE SURVEY

Alexandra Rivero-Garca (2016) the method is based both on the verification votes of the users, and on their profiles and trust levels. Each user is allocated trust level depending on its previous behavior. The proposal is founded on assumption that the system will be run in every driver mobile device. [13]

Xiao Ya (2015) value of reputation which reflects trustworthiness of node is broadcasted and calculated through intersection nodes, it protocol includes location detection [14] technique to attack area faking conduct of nodes malicious. [14].

Wenjia Li (2015) ART management scheme is suggested for VANETs that is able to cope and detect using malicious attacks and evaluate trustworthiness of both cell nodes and data in VANETs.[15]

Kapil Sharma (2015) Trust based location finding in VANET is needed to deter transmission of messages malicious or selfish and enable other vehicles to filter out such data. the application of Dempster-Shafer theorem (DST) for computing trust in environment for VANET for location finding is presented. [16]

Amel Ltif (2015) The concept of vehicle Active that combines power of V2V technologies and intelligence ambient is introduced. For ready support, propose new model for administration trust for VANET established on coordinated effort between "Active vehicles" to upgrade wellbeing states and to cut using spread of false warnings by vehicular network. [17]

Sanoop Mallissery (2014) Novel architecture is suggested for trusted substructure using combination of short time certificate and Merkle Signature Scheme. Safe VANET communication is achieved using psuedo ID created by vehicle and factor of short certificate through trusted infrastructure that grants private public key pairs according to priority of messages exchanged in architecture. [18]

Nikhil Kapade (2014) Recently various routing protocol has been suggested for message forwarding like proportional, Frame and receipt counting. it is needed to give node some incentive to forward message. Nevertheless for higher vehicle density area, they have not addressed load balancing factor for data forwarding. [19]

Kavitha. M (2013) communication between vehicles is used for comfort, entertainment and safety. Presentation of communiqué depends on how improved routing takes place in network. Routing of data depends on routing protocols being used in network. [20]

Qiwu Wu (2013) The suggested protocol not only improves security of routing, but also has lower time complexity. Paper puts forward trusted protocol routing in VANET Based on GeoDTN+Nav routing protocol. Experimental outcomes and analysis show that suggested protocol has achieved good performance in removal ratio of nodes malicious, correct reception ratio of packet and the message payload. [21]

G. Gowtham (2012) communication between nodes takes place in secured way through using security algorithms similar ECDSA and TESLA. VANET uses hardware is known as TPM to provide secured nodes between communication. For safe communication between nodes, node should trust communicating node before communication using this and if it is found legal then communicate using this. [22]

IV. PROBLEM STATEMENT

The vehicular network is a growing area of research, due to its functionality there are lots of fundamental security issues. This network easily threatened by attack, lots of works already done in a field of VANET but all have some problems. In existing work all responsibility of trust assignment gives to law executer if LE itself becomes malicious node than trust calculation is going to be wrong, for providing more security data send by nodes using encryption technique. Hashing is used for encryption and decryption, hashing is not secure technique because of its keys easily hacked by hackers. Overcome this problem we gave RSU based centralized and AES based security technique.

V. PROPOSED WORK

Security is the main concern of any other network because of if attacks apply in networks than users suffer and quality of service is down when we talk about VANET which is highly moveable or infrastructure of VANET change frequently in this network security is main concern because if its flexible and secure passengers feel convenient to travel. Trust is the most important area, to build trust between vehicles we apply behavior based technique.

Behavior based technique is one of the most common and easy to use. in this method first we check that if one node sends data and how many time it's get reply we understand this concept like if a node sends again and again false message and did not get the reply because requested area or node does not exist this is called flooding attack so secure network by this attack we check RREQ of every node so that if count of RREQ is greater than threshold we decrease the trust value of node now we check the whole thing like receiving packet forwarding packet and number of drop packets so that we increase or decrease the trust of nodes. By using trust we only save network by the active attack for passive attacks this technique does not work.

Passive attacks are more harmful to the network because intruder node modifies the data and send to the destination node for escape or prevent our network by these attacks we apply the propelled encryption standard technique.

Algorithm

```
Step1: network start
Step2: if(sendpacketcount>>threshhold){
            Decrease trust   go to step3}
   Else
       Increase trust  go to step3 }
Step3: if(receivepacket>=forward&&drop>>threshhold){
           Decrease trust }
      Else
          Increase trust
Step4: create array of trust node
Step5: apply AES
```

AES(Advance Encryption Technique)

The AES cipher is practically Equal to the block cipher, rijndael cipher developed with two exceptional belgian cryptographers, J. Daemen and V. Rijmen. The algorithm defined via AES is a symmetric-key algorithm, value the same key is used for both data encrypting and decrypting (figure 1). The internal rounds number of the cipher is a function of the key length. The quite a lot of rounds for 128- bit key's 10. Not like its predecessor DES, AES does no longer use a feistel network. Feistel networks don't encrypt an entire block per iteration, e.G., in DES, 64/2 = 32 bits are encrypted in one round. AES, on the other distinct hand, encrypts all 128 bits in a single new release. This is the one motive why it has a comparably little number of rounds.

AES Encryption:

The encryption procedure in the AES contains following level:

(i) Do the one-time initialization procedure:
(a) Expand 16-byte key to found the actual Key Block to be used.
(b) Do one time initialization of the 16-byte plain text block (called State).
(c) XOR the state with the key block.

(ii) For all round do the following:
(a) Using S-Box to all of the plain text bytes.
(b) Rotate row k of the plain text block (i.e. state) by k bytes.
(c) Perform mix columns process.
(d) XOR the state with the key block.

VI. SIMULATION RESULT

A. Packet delivery ratio:

The PDR is described as the ratio of data packets bought by way of approach for the destinations to these produced from the sources. Mathematically, it may be outlined as:

PDR= S1÷ S2

where, S1 is the sum of data packets got with the aid of the each destinations and S2 is the sum of data packets produced with the guide of the each source. The graphs exhibit the fraction of data packets which might be efficaciously delivered in the course of simulation time versus the number of nodes.

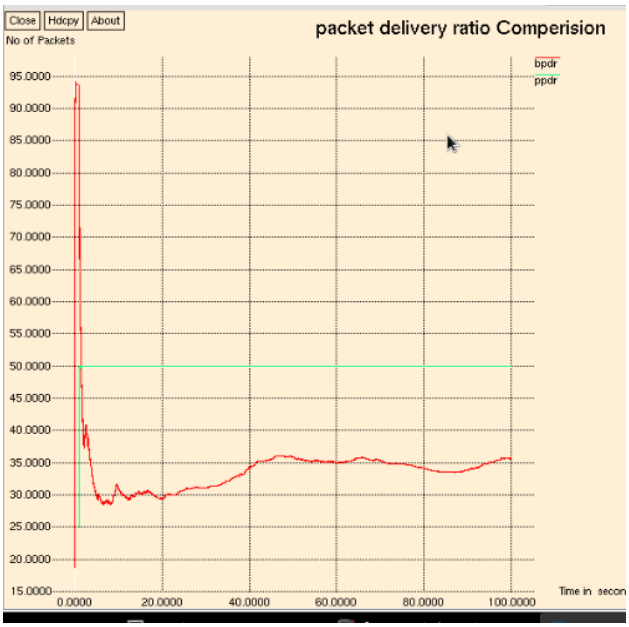

Fig 2: Shows Comparison between base (red) and Proposed (green) values in PDR.

B. Routing Overhead:

Routing overhead refers to metadata and network routing information despatched with the aid of application, which makes use of a component of the available bandwidth of communications protocols. This additional information, make up the procedure headers and a purpose-specific data are referred to as transparency, because it doesn't throw into the Substance of the discussion. Protocol overhead may also be expressed as a percentage of non-application bytes (protocol and body synchronization) divided by the whole number of bytes within the message.

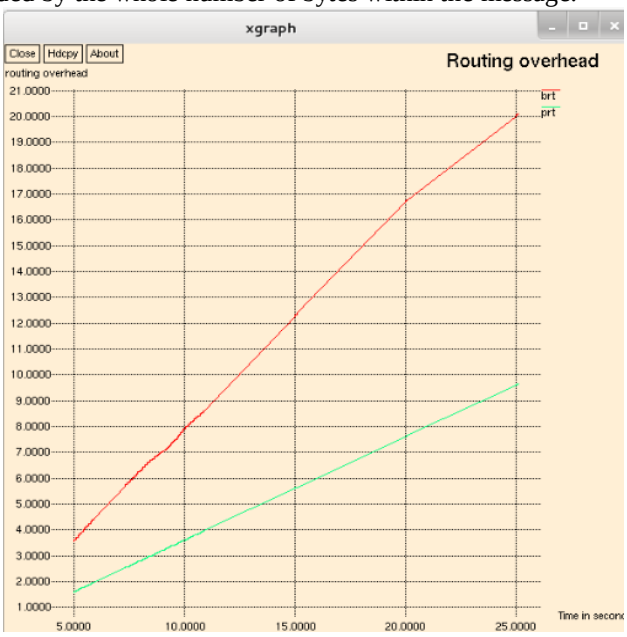

Fig 3: Comparison between base and proposed values in routing overhead.

C. Throughput:

It is characterized as the aggregate number of packets delivered over the total simulation time. The throughput comparison shows that the three algorithms performance margins are very close under traffic load of 50 and 100 nodes in MANET scenario and have large margins when the number of nodes increases to 200. Mathematically, it can be defined as:

Throughput= N/1000

Where N is the number of bits bought effectively by using all destinations.

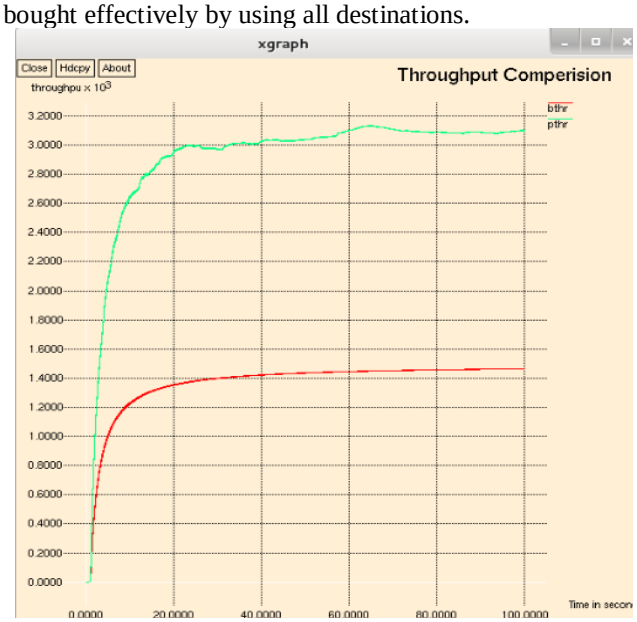

Fig 4: Shows Comparison between base (red) and Proposed (green) values in Throughput.

VII. CONCLUSION

VANETs are the promising process to furnish defense and different functions to the drivers as good as passengers. It becomes a key element of the intelligent transport system. AES is an iterative as a substitute than Feistel cipher. It's centered on 'substitution–permutation network'. It includes of a series of linked operations, some of which contain replacing inputs via specific outputs (substitutions) and others contain shuffling bits round (permutations). In this paper apply behavior based technique for passive attack.

REFERENCES

[1] S.Al-Sultan, M.M. Al-Doori ,A.H. Al-Bayatti , H. Zedan," A comprehensive survey on vehicular Ad Hoc network," Journal of Network and Computer Applications, Vol. 37, pp.380–392, 2014.

[2] H.Hartenstein, K.P.Laberteaux, "A tutorial survey on vehicular ad hoc networks," Communications Magazine, IEEE, Vol.46, Issue. 6, pp. 164 - 171, 2008.

[3] P.Pereira, A. Casaca, J.Rodrigues, V. Soares, J. Triay, C.Cervello-Pastor," From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks," Communications Surveys & Tutorials, IEEE, Vol.14,Issue.4, pp. 1166 - 1182,2012.

[4] M.L.Sichitiu, NC.Raleigh, M. Kihl, "Inter-vehicle communication systems: a survey," Communications Surveys & Tutorials, IEEE, Vol 10, Issue. 2, pp.88 – 105, 2008.

[5] J.Harri, F.Filali, C.Bonnet," Mobility models for vehicular ad hoc networks: a survey and taxonomy," Communications Surveys & Tutorials, IEEE, Vol. 11 , Issue: 4, pp.19 – 41, 2009.

[6] J.Jakubiak, Y.Koucheryavy, "State of the Art and Research Challenges for VANETs,"Proc. of 5th IEEE Consumer Communications and Networking Conference, pp.912-916, 2008.

[7] M.Faezipour, M. Nourani, A.Saeed, S.Addepalli, "Progress and challenges in intelligent vehicle area networks," Communications of the ACM, Vol.55, Issue 2, pp. 90-100, 2012.

[8] T. Kosch, I. Kulp, M. Bechler, M. Strassberger, B. Weyl, and R. Lasowski, "Communication architecture for cooperative systems in Europe," Communications Magazine, IEEE, Vol.47, Issue.5, pp.116–125, 2009.

[9] [9] Qingwen Zhao, Yanmin Zhu, Chao Chen, Hongzi Zhu, Bo Li, "When 3G Meets VANET: 3GAssisted Data Delivery in VANETs," Sensors Journal, IEEE, Vol.13, Issue.10, pp.3575, 3584, 2013.

[10] S.Panichpapiboon, W. Pattara-atikom, "A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks," Communications Surveys & Tutorials, IEEE, Vol.14, Issue.3, pp. 784 - 798, 2012.

[11] Zhen Huang, Sushmita Ruj, Marcos A. Cavenaghi, Milos Stojmenovic and Amiya Nayak," A social network method to trust management in VANETs", Springer Science, 2012.

[12] Raya M, Shokri R, Hubaux J-P (2010) On the tradeoff between trust and privacy in wireless ad hoc networks. In: ACM WISEC, pp 75–80

[13] Minhas UF, Zhang J, Tran T, Cohen R (2010) Towards expanded trust management for agents in vehicular ad-hoc networks. IJCITP 5(1):3–15

[14] Alexandra Rivero-Garcıa, Ivan Santos-Gonz alez, Pino Caballero-Gil and C andido Caballero-Gil. VANET event verification based on user trust. 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing. PP: 313-316

[15] Xiao Ya, Zheng Shihui. Trusted GPSR protocol without reputation faking in VANET. School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China. PP: 22-31

[16] Wenjia Li. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. PP:1-10

[17] Kapil Sharma, Brijesh Kumar Chaurasia. Trust Based Location Finding Mechanism in VANET using DST. 2015 Fifth International Conference on Communication Systems and Network Technologies. PP:763-766

[18] Amel Ltifi , Ahmed Zouinkhi , Mohamed Salim Bouhlel. Trust-based Scheme for Alert Spreading in VANET. The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015). PP:282-289

[19] Sanoop Mallissery, Manohara Pai M.M., Smitha A., Radhika M. Pai, Joseph Mouzna. ,IMPROVIZING THE PUBLIC KEY INFRASTRUCTURE TO BUILD TRUST ARCHICTURE FOR VANET BY USING SHORT-TIME CERTIFIED MANAGEMENT AND MERKLE SIGNATURE SCHEME. 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE). Pp:146-151

[20] Nikhil Kapade. TLC: Trust point Load Balancing Method using Coalitional Game Theory for Message Forwarding in VANET. 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN). PP: 160-164

[21] Kavitha . M , Shrikant S.Tangade , SunilKumar S.Manvi. Distributed Trust & Time Management Strategy in VANETs. IEEE – 31661. PP:1-6

[22] Qiwu Wu, Qingzi Liu. A TRUSTED ROUTING PROTOCOL BASED ON BAYESIAN IN VANET. University of Armed Police Force, P. R. China. PP: 1-4

[23] G.Gowtham , E.Samlinson. A SECURED TRUST CREATION IN V ANET ENVIRONMENT USING RANDOM PASSWORD GENERATOR. 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]. PP:781-784

