e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

IMPROVED NAVIGATION AND SECURITY USING TEAM ALGORITHM IN VANET

S.Saranya[1],M.Sharmila Devi[2], M.Sharmila[3], K.Yoganandhini[4]
[1] *InformationTechnology,VivekanandhaCollege of Engineering for Women,*
[2]*InformationTechnology,VivekanandhaCollegeofEngineering forWomen,*
[3]*InformationTechnology, Vivekanandha College of EngineeringforWomen,*
[4] *Information Technology, Vivekanandha College of Engineering for Women*

Abstract---The security of Vehicular Ad hoc Networks (VANETs) is receiving a significant amount of attention in the field of wireless mobile networking because VANETs are vulnerable to malicious attacks. A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The vehicular nodes communicate with other vehicle nodes and share the messages. By receiving GPS signals, the device can determine its current location and then find the geographically shortest route to a certain destination based on a local map database. A number of secure authentication schemes based on asymmetric cryptography have been proposed to prevent such attacks. Hence, this still calls for an efficient authentication scheme for VANETs. A new technique of decentralized lightweight authentication scheme called as Trust-Extended Authentication Mechanism (TEAM) for Vehicle-to-Vehicle communication networks. TEAM adopts the concept of transitive trust relationships to improve the performance of the authentication procedure and only needs a few storage spaces. Moreover, TEAM satisfies the following security requirements: anonymity, location privacy, mutual authentication, forgery attack resistance, modification attack resistance, replay attack resistance, no clock synchronization problem, no verification table, fast error detection, perfect forward secrecy, man-in-the-middle attack resistance, and session key agreement.

Keywords-Authentication, decentralized, lightweight, trust extended authentication mechanism, vehicular ad hoc networks (VANET).

I INTRODUCTION

Vehicular Ad hoc Networks (VANETs) is attracted by increasing the attention from both industry and academia. The major components of a VANET are the wireless On-Board Unit (OBU), the Road Side Unit (RSU), and the Authentication Server (AS). OBUs are installed in vehicles to provide wireless communication capability, while RSUs are deployed on intersections or hotspots as an infrastructure to provide information or access to the Internet for vehicles within their radio coverage. The AS is responsible for installing the secure parameters in the OBU to authenticate the user. The dedicated short range communication system supports two kinds of communication environments: Vehicle-to-Infrastructure (V2I) and Vehicle-to Vehicle (V2V) communications. The security issue in VANETs has become a hot topic, and then many researchers provide the V2I and V2V authentication mechanisms to protect valid users. However, the design for an efficient V2V authentication mechanism is more challenge than that for V2I authentication mechanism in VANETs because the vehicle cannot be authenticated via the infrastructure directly in V2V communications. Therefore, it focuses on V2V network environments and proposes an efficient authentication scheme. To address the above need, to propose a decentralized authentication scheme, called TEAM, for V2V communication networks. There exists no centralized authority to perform the authentication procedures of vehicles. TEAM is a lightweight authentication scheme because it only uses an XOR operation and a hash function. Although TEAM needs low computation cost, it still satisfies the following security requirements: anonymity, location privacy, mutual authentication, resistance to stolen-verified attacks, forgery attacks,

modification attacks and replay attacks, as well as no clock synchronization problem, fast error detection, perfect forward secrecy, man -in- the-middle attack resistance, and session key agreement. Moreover, this scheme only requires a few storage spaces than other schemes because the vehicle does not need to store the authentication information (e.g., public key) of T. To add the adversary model discussion, secure communication, password change, key update, and key revocation procedures in this enhanced version. The analysis of computational and storage costs of TEAM, and then to use the (NS-2) network simulator to evaluate the performance of TEAM.

II EXISTING SYSTEM

Vehicular Ad-hoc Networks comprises of vehicular nodes that are equipped with wireless communication modules. A VANET is composed of three components: OBUs equipped in moving vehicles, fixed RSUs, and a central Trusted Authority (TA).The OBUs are the wireless units fitted in the vehicles such as cars to enable the wireless communication feature. The RSUs are used as access points for Vehicular node as the moving vehicular node can deliver or access the messages, Internet.etc. The TA authenticates each and every vehicular node using digitally signed Certificates. Finding a route to a certain unknown destination is a common experience for all drivers and in the old days, a driver usually refers to a hard copy of the local map.With the introduction of Global Positioning System (GPS), GPS-based navigation systems become popular and reduce the drawbacks of referring hard copy of the local map. By receiving GPS signals, the device can determine its current location and then find the geographically shortest route to a certain destination based on a local map database.

III LITERATURE SURVEY

The security of Vehicular Ad Hoc Networks (VANET) has mostly directed the attention of today research efforts, while comprehensive solutions to protect the network from adversary and attacks **[1].** Communication messages in vehicular ad hoc networks (VANET) can be used to locate and track vehicles. While tracking can be beneficial for vehicular node navigation, it can also lead to threats on location privacy of vehicular node user **[2].** Vehicular Ad Hoc Networks (VANETs) require a mechanism to help authenticate messages, identify valid vehicular nodes, and remove malevolent vehicular nodes. A Public Key Infrastructure (PKI) can provide this functionality using certificates and fixed public keys **[3].** In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext **[4].** In a proxy re-encryption scheme a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. A number of solutions have been proposed in the public-key setting **[5].** VANET improves road safety and traffic conditions via the vehicular node exchange the traffic information with other vehicular nodes and some infrastructures immediately. Ensuring that exchange messages are secure, trustworthy and protect user privacy are important issues **[6].** Receiver-location privacy is an important security requirement in privacy-preserving Vehicular Ad hoc Networks (VANETs), yet the unavailable receiver's location information makes many existing packet forwarding protocols inefficient in VANETs **[7].** Introduce a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves **[8].**

IV PROPOSED SYSTEM

A TEAM is a decentralized authentication scheme, and the LEs need not to keep the authentication information of the entire vehicular nodes. The proposed scheme involves eight procedures: initial registration, login, general authentication, password change, trust-extended authentication, key update, key revocation, and secure communication. Before a vehicular node can join a VANET, its OBU must

register with the AS. When a vehicular node wants to access the service, it has to perform the login procedure. Next, the OBU checks the authentication state itself (i.e., the lifetime of the key). If the lifetime of the key is reduced to zero, the vehicle is mistrustful, and vice versa. The trustful vehicular nodes assist other MVs in performing the authentication procedure or communicate with other trustful vehicular nodes (i.e., secure communication procedure) to access the Internet. The trustful vehicular nodes perform the key update procedure with the LE when the key lifetime is below the predefined threshold. Moreover, the password change procedure for user friendly was considered.The state of the LE does not change because the LE is always trustful. Many related works point out that the system of vehicular node is better protected than the general mobile device (e.g. smart phone, etc.). Therefore, to assume that each vehicular node's OBU is equipped with security hardware (e.g., trusted platform module), including an Event Data Recorder (EDR), and a Tamper-Proof Device (TPD) so that an attacker cannot obtain information about the vehicular node from the OBU. The EDR is responsible for recording important data about the vehicular node, such as the location, time, preload secret key, and access log. The TPD provides the cryptographic processing capabilities. Finally, in this system assume that the time of every vehicular node is synchronous via GPS device.

Benefits of TEAM

TEAM adopts the concept of transitive trust relationships to improve the performance of the authentication procedure.TEAM satisfies the following security requirements: anonymity, location privacy, mutual authentication to prevent spoofing attacks, forgery attacks, modification attacks and replay attacks, as well as no clock synchronization problem, no verification table, fast error detection, and session key agreement.

MISTRUSTFUL **TRUSTFUL**

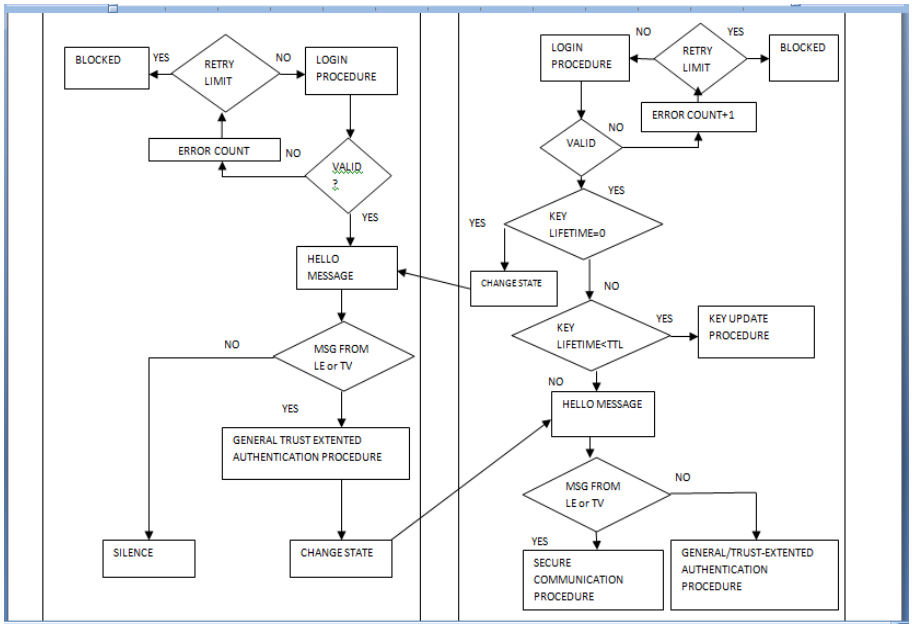

Fig 1 Operations of MISTRUSTFUL/TRUSTFUL Vehicle Implementation

V IMPLEMENTATION

In VANETs, vehicular node can be classified into to the following roles: a Law Executor (LE), a MV, and a TV as illustrated in Fig. 5. An LE, such as police car or authorized public transportation (e.g.,

buses), acts like a mobile AS. Moreover, the LE is trustful permanently. A normal vehicular node is regarded as trustful if it can be authenticated successfully; it is deemed to be mistrustful. In addition, the TV becomes the MV when the key lifetime is over. To provide a secure communication environment, the OBU should be authenticated successfully before it can access the service. However, in V2V communication networks, as the number of LEs is finite, an LE is not always in the vicinity of the OBU. Even if the user is well meaning, the vehicular node must still wait for the nearest LE and then perform the authentication procedure. Hence, there is an urgent need for an efficient authentication scheme. In this scheme a TEAM to improve the performance of the authentication procedure in V2V communication networks. The TEAM is based on the concept of transitive trust relationships. Initially, there are three vehicular nodes in a VANET: a trustful LE and two other MVs carrying OBUs .The state of the first mistrustful OBU (i.e., OBUi) becomes trustful and obtains the sufficient authorized parameter to authorize other mistrustful OBUs when it is authenticated successfully. Then, it plays the LE role temporarily to assist with the authentication procedure of OBU. Thus, the other mistrustful OBUs can be authenticated by any trustful OBU without necessarily finding an LE and all vehicular nodes in a VANET can complete the authentication procedure quickly.

VI RESULTS

A. Vehicular Ad-hoc Network Creation

In this module, a vehicular network is created. All the vehicular nodes are randomly deployed in the network area. All the vehicular nodes are connected using wireless links and they can communicate with each other using wireless medium. Since our network is a vehicular network, nodes are assigned with mobility (movement). All the vehicular nodes are moving in the network area with inconsistent speed.

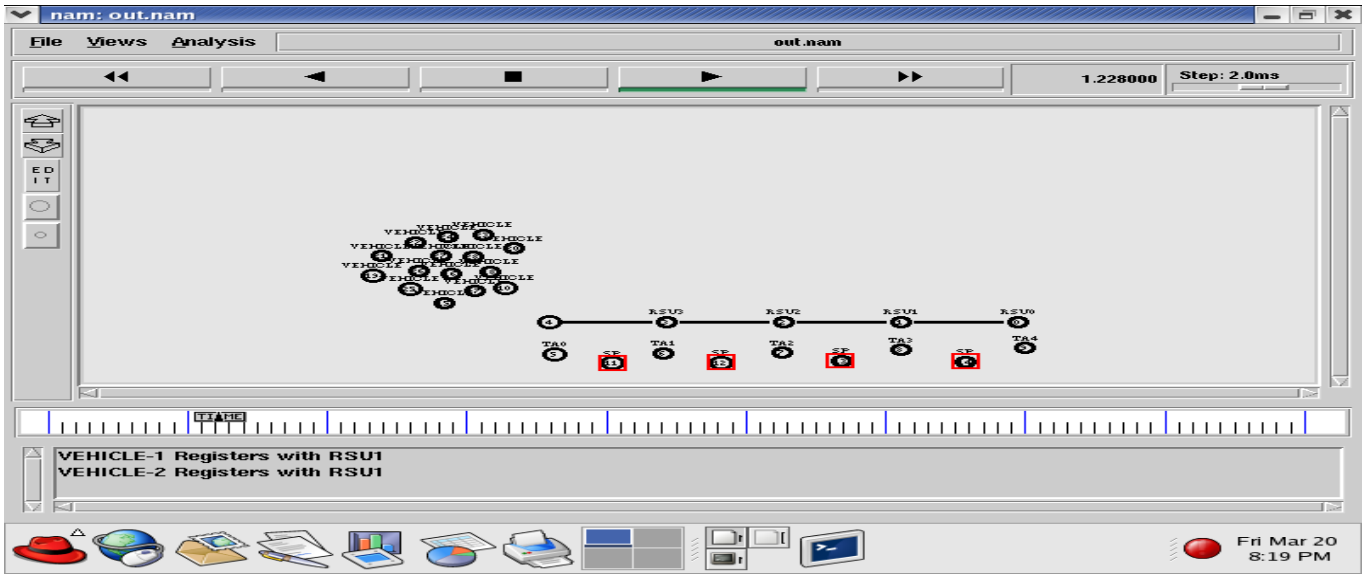

Fig 2 Vehicular Ad-hoc Network Creation

B. Performance Analysis

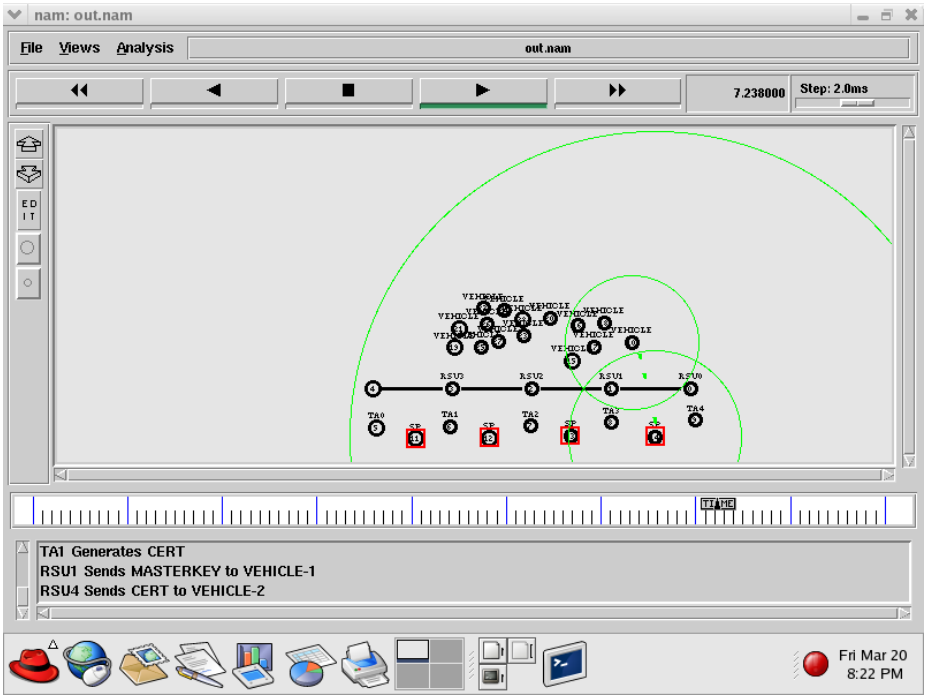

Fig 3 Performance Analysis

In this module, the performance of the routing is analyzed. Communication delay, traffic delay packet loss are analyzed. Throughput, delay, energy consumption are the basic parameters. Road side unit sends MASTERKEY to vehicular nodes and the next road side unit sends certificates to next vehicular nodes.

C. Implementation of VSPN

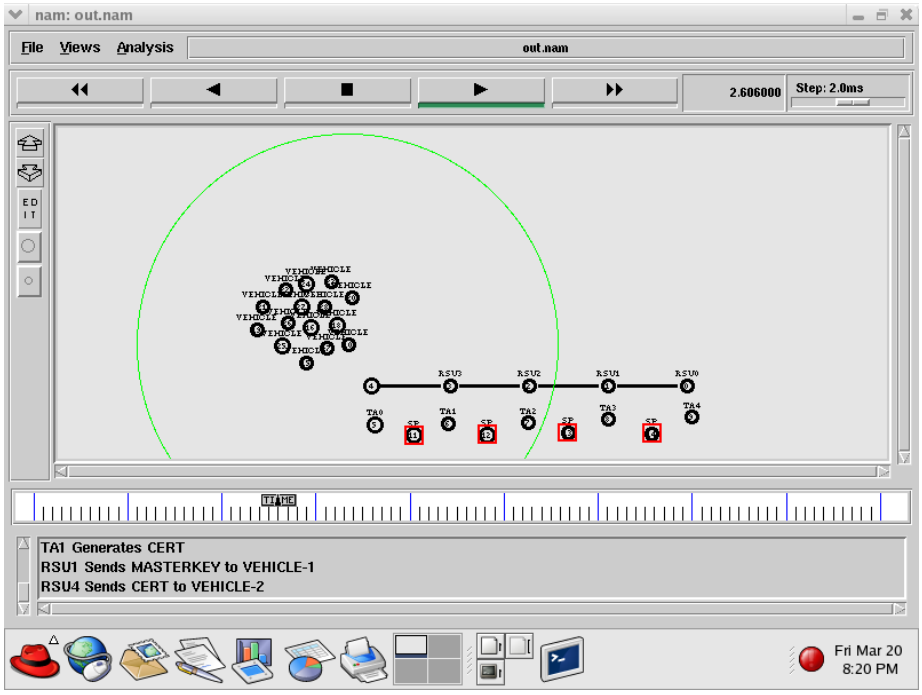

Fig 4 Implementation of VSPN

In this module, VSPN is implemented. VSPN makes use of the collected data to provide navigation service to drivers. Based on the destination and the current location of the driver (the query), the system can automatically search for a route that yields minimum traveling delay in a distributed manner using the online information of the road condition. TA generates public and private keys for the vehicular nodes.

D. Execution of TEAM

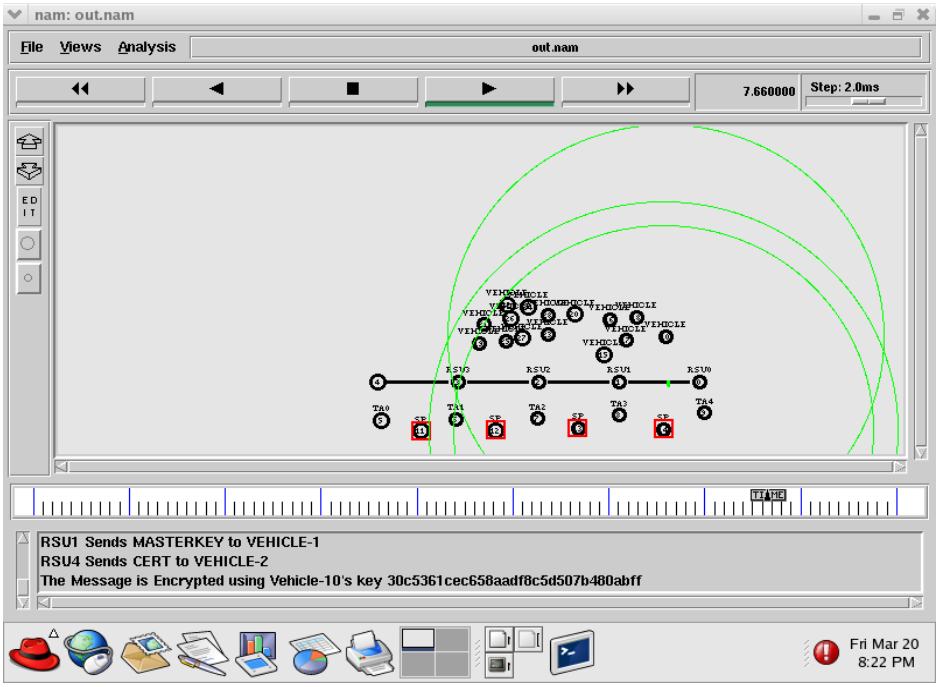

Fig 5 Execution of TEAM

When a vehicular node wants to access the service, it has to perform the login procedure.Next, the OBU checks the authentication state itself (i.e., the lifetime of the key).If the lifetime of the key is reduced to zero, the vehicular node is mistrustful, and vice versa.The MV performs the general or trust-extended authentication procedure to be authenticated.

VII CONCLUSION

A technique of decentralized lightweight authentication scheme called TEAM to protect valid users in VANETs from malicious attacks. The amount of cryptographic calculation under TEAM was substantially less than in existing schemes because it only used an XOR operation and a hash function. Moreover, TEAM is based on the concept of transitive trust relationships to improve the performance of theauthentication procedure.

REFERENCES

[1] G. Samara, W. Al-Salihy, R.Sures, (2010) "Security Issues andChallenges of Vehicular Ad Hoc Networks (VANET)," Proc. IEEEFourth Int'l Conf., pp. 393-398.

[2] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran,(2007)"AMOEBA: Robust Location Privacy Scheme for VANET," IEEEJ. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589.

[3] A. Studer,E. Shi, F. Bai, and A. Perrig, (2009)"TACKing TogetherEfficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE Sixth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad HocComm. and Networks (SECON '09), pp. 1-9.

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,(2005) "ImprovedProxy Re-Encryption Schemes with Applications to SecureDistributed Storage," Proc. 12th Ann. Network and DistributedSystems Security Symp.(NDSS).
[5] M. Green and G. Ateniese,(2007) "Identity-Based Proxy Re-encryption,"Proc. Applied Cryptography and Network Security Conf.
[6] R. Hwang, Y. Hsiao, and Y. Liu,(2011) "Secure Communication Scheme of VANET with Privacy Preserving," Proc. IEEE 17th Int'l Conf. Parallel and Distributed Systems (ICPADS '11), pp. 654-659.
[7] X. Lin, R. Lu, X. Liang, and X. Shen,(2011) "STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in VANETs," Proc. IEEE INFOCOM '11,pp. 2147-2155.
[8] D. Boneh, B. Lynn, and H. Shacham,(2001) "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf.pp. 514-532.

