FORTIFY MANETs FROM INVASION USING HYBRID CRYPTOGRAPHIC TECHNIQUES

Amudha Bharathi.B[1] and Dr.S.Usha[2]

[1] PG Student, ME Computer and Communication, Sri Sairam Engineering College, Chennai-44.

[2] Associate Professor,Department of IT, Sri Sairam Engineering College, Chennai-44.

amudha.bhaskaran@gmail.com

usha_sakthivel@yahoo.co.in

ABSTRACT

Wireless Networks are always preferred from the first day of invention due to mobility and scalability. Mobile Ad hoc NETwork(MANET) has become one of the most wireless communication mechanisms. Security is the problem in wireless networks. The lacking of security leads to occurrence of Intrusion. The Pre-Existing Research, an intrusion detection system named EAACK is designed but it increase the network overhead by digital signature. In this paper we propose by adopting hybrid cryptographic techniques reduce the network overhead and to eliminate the requirement of predistributed keys by the key exchange mechanisms.

Keywords: MANET, EAACK, Hybrid Cryptography, RSA

1. INTRODUCTION

Mobile Ad hoc NETwork(MANET) is a type of Wireless ad hoc network. Among all the contemporary wireless Networks MANET is one of the most and unique application. A Mobile Ad hoc NETwork or MANET consist of a group of cooperating wireless mobile host that dynamically construct of short lived and self configuring network. The mobile host can be cell phone, PDAs and laptops. As MANET does not require any fixed infrastructure. With the self configuring the nodes has the ability among critical mission applications like military and emergency recovery. One advantage of wireless network is the ability to transmit data among users in common area while remaining mobile. Security is the problem in wireless networks. The lacking of security leads to occurrence of Intrusion. The architecture of MANET is shown in the figure 1

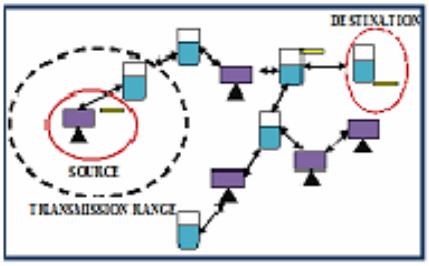


Fig 1 MANET Architecture

2.RELATED WORK

An Existing solution states that an intrusion detection system called Enhanced Adaptive ACKnowledgement (EAACK) [1]. This system comprises three major parts ACK(ACKnowledgement),SecureACK(SACK), Misbehaviour Report Authentication(MRA).The concept of this system is to eliminate the weakness of Watchdog scheme namely false Misbehaviour, limited transmission power and receiver collision. The ACK method is a basic end-to-end acknowledgement scheme. It is used to reduce network overhead when no network misbehavior is detected. The Secure ACK method is the enhanced version of TWOACK. The function of TWOACK scheme [4] is send two hop acknowledgement by the destination for every packet to the sender within a predefined time period. If the acknowledgement is not received means that node is said to be malicious .Another scheme called misbehavior report authentication. The function of this scheme is to authenticate. It is used to detect the malicious node although a false misbehavior report is existed. In EAACK, the network overhead is more because of Digital signature [2] but performance is better.

3.PROPOSED WORK

To secure MANET acknowledgement based methods are employed. In this paper by using the hybrid cryptographic method [7] manet is to be fortified and to eliminate the requirement of pre distributed keys. The Hybrid Cryptographic are consist of Advanced Encryption Standard(AES), Rivest, Shamir and Adelman(RSA), Digital Signature Standard(DSS) and Secure Hash Algorithm(SHA). AES algorithm is used to generate session key. RSA algorithm is used to generate public key and private key.DSS algorithm is used to generate signature key. SHA algorithm is used to generate hash value. The Architecture of invasion system is shown in the figure 2

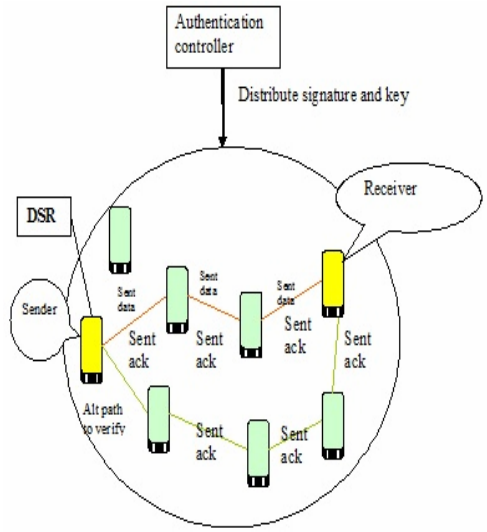


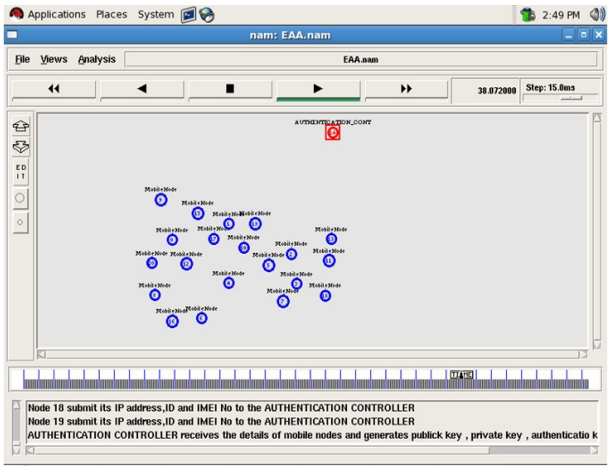
Fig 2 Architecture

In the development of our paper Authentication Controller is present it act as a server. The function of Authentication Controller is to generate key to all nodes in the network, key revocation and session establishment. At the initial stage all the nodes in the network is

register in the Authentication Controller. For the key generation it use hybrid cryptographic method of both symmetric and asymmetric key as both private and public key and a common key is called authentication key. The public and private key is different for all nodes in the network. Public key is used for encryption. Private key is used for Decryption. Authentication key is used for Verification. Then the key is distributed to all the nodes in network. The source node determine path to destination with the Dynamic Source Routing protocol. For the transmission the session is established by authentication controller by check the id and value of the destination. If it authenticated means authentication controller provide public key certificate and value to source. Then source send request to receiver after receiving the request destination send the request to authentication controller with the parameter of session key, id and secret message. Once these parameters are authenticated the session is established between the source and destination. After these the message is transmitted from source to destination. Hash value is encrypted using receiver's public key for the verification. Key revocation is used at the time of any node is present in network deployment stage after that it moving out of communication range means its key and id is terminated by authentication controller. Again it enter in the network means a new key and is generated this process is termed as key revocation. By these mechanisms manet is secure from invasion.

4.IMPLEMENTATION

Initial stage of this paper is node authentication and key generation.The network is deployed by using NS 2.34 and linux 5.4 as operating system. Authentication Controller distribute access id to all the mobile nodes in the network after receive this id mobile nodes submit its id, IMEI Number and IP address to authentication controller. Then it saves these details and generate the key Using RSA algorithm. This process is implementation is shown in the figure 3



5.CONCLUSION

To secure manet from intrusion acknowledgement based mechanism produce delay and performance is less. For eliminate this issues hybrid cryptographic method is employed in this paper it reduce the network overhead caused by digital signature and the requirement of predistributed keys. By the authentication

controller this process are carried out. This approach easily find out the malicious node and increase the performance of the network.

6.REFERENCES

[1]. Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transaction on Industrial Electronics, Vol. 60, No. 3, March 2013.

[2].N.Kang, E.Shakshuki and T.Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[3]. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[4].K.Liu,J.Deng, P.K.Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007

[5]. N.Nasser and Y.Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int.Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[6]. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf.Perform., Comput., Commun., 2004, pp. 747–752.

[7].E.Kamaraj, s.Karthikeyan, M.Hemalatha, "A Design of Security Protocol using Hybrid Encryption Technique," International Journal of the Computer Vol 17.No.1, 2009,pp 78-86.

[8]. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[9]. A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf.Pervasive Comput. Commun., 2005, pp. 191–199.