ISSN:0975-9646

R. Vedhavarshini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3309 - 3311

Efficient Data Packet Transmission in MANET Using Enhanced Hybrid Cryptographic Technique

R. Vedhavarshini [1], T. Anand [2]

[1] *Master of Computer Science and Engineering*
K.S.R. College of Engineering, Tiruchengode, India

[2]*Assistant Professor, Department of CSE*
K.S.R. College of Engineering, Tiruchengode, India

Abstract-Mobile Ad hoc Network (MANET) consist of independent mobile nodes without any fixed infrastructure. All mobile nodes cooperatively transfer their data packets to other mobile nodes in the network within their transmission range. Mobile nodes depend on intermediate nodes when transmission range beyond limit (i.e), multi hop network. Various attacks is possible in manet due to its open environment and dynamic nature. Security is important to avoid those attacks. This paper analysis various Intrusion Detection System (IDS) to avoid packet data loss in network.

Keywords: IDS, MANET, Packet Drop Attack, Security

I. INTRODUCTION

MANET (Mobile Ad hoc Network) is an infrastructure less wireless network where mobile nodes can move freely and can form network. These networks don't have infrastructure and the communication occurs within the transmission range due to limited resource of energy for each node. Routing Protocols play an important role in MANET for connectivity between nodes for transfer of data packets between each nodes in the network and can be classified into Proactive routing protocols, Reactive routing protocols and Hybrid routing protocols. Proactive routing protocols uses routing table and exchanges link information in between nodes. Reactive protocol establishes routes only when nodes are ready to communicate means nodes does not exchange routing information. Hybrid combines the features of both proactive and reactive routing protocols. Due to the absence of centralized authority MANET is more susceptible to attacks by selfish nodes or malicious nodes.

II. ROUTING ATTACKS IN MANETS

Routing plays a very important role in MANETS. It can also be easily misused, leading to various types of attack in the network. Routing protocols in general are more easily attacked by malicious nodes.

These protocols are usually not designed with security function and often they are very vulnerable to node misbehavior attacks. It is true for MANET routing protocols because they are designed for minimizing the level of overhead and for allowing every node to participate in the routing process.

Various routing attacks [9] caused by attackers in MANET are:

a) Black Hole Attack

In this attack a malicious node makes use of routing protocols to misrepresents that it having the shortest and fresh enough route to destination without checking the availability of routes and drops data packets without forwarding further, thereby degrading network performance.

b) Wormhole Attack

In a wormhole attack [9], an attacker receives packets at one end point in the network, tunnels data packets to another end point in the network, and then replays them into the network from that point. This tunnel between these end points cause two colluding attacks is known as a wormhole.

c) Replay Attack

An attacker which performs a replay attack is retransmitted the valid data repeatedly to cause network routing traffic that has been captured previously. This attack usually aims at the freshness of routes.

d) Gray-hole Attack

This attack is also known as routing misbehavior attack which leads to dropping of messages.

It has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain conditions.

e) Flooding Attack

In flooding attack multiple RREQ'S are sent from void IP addresses if the scope of the IP address is known else random IP addresses are chosen and the network is flooded with a large number of RREQ'S hence it is named flooding.

All these attacks clearly indicate loss of packet delivery to the end point. It is referred as Packet Drop Attack.

III. DATA PACKET DROP ATTACK

A Data Packet is dropped [15] due to following reasons such as:

- **Unsteadiness of Medium**

  Packet may be dropped due to corruption and broken links

- **Geneuiness of node**
  Packet may be dropped due to overflow of transmission queue and lack of energy resources.
- **Selfish node**
  Data packets are dropped due to saving of its own energy resources.
- **Malicious node**
  Packet [13] is dropped due to malignant act of a node.

IV. INTRUSION DETECTION IN MANET

Intrusion Detection System (IDS) [14] is used to detect the malicious nodes and to avoid packet drop in MANET. IDS should be cooperative and energy efficient for a constant changing topology and limited battery of mobile nodes in MANET . It can improve packet delivery ratio and to reduce routing overhead in MANET.

The properties of IDS in MANET are:

- IDS might utilize minimize resources to provide security to the mobile nodes.
- IDS must detect intrusion on each mobile node and have run-time efficiency.
  Several techniques available for detection of misbehaving nodes in MANET. They are :
- **Reputation-Based Technique**
  In this network nodes collectively detect and declare the misbehaviour of a suspicious mobile node. Such a declaration is then propagated throughout the entire network, so that the misbehaving node will be cut off from the rest of the wireless network.
  Eg: Watchdog and Pathrater.
- **Credit Based Technique**
  The basic idea of credit based technique is to provide credits for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up.
- **Acknowledgement Based Technique**
  It rely on the reception of an
  Acknowledgment from a mobile node to verify that a packet has been forwarded to it.
  Eg: TWOACK, AACK, EAACK

V. METHODS TO DETECT INTRUSION IN MANET

Watchdog and Pathrater [1] form the basis for many packet dropping detection techniques. The first technique is the Watchdog that identifies misbehaving mobile nodes and second technique is the Pathrater that helps routing protocols to avoid those mobile nodes used in future. But, it can't detect malicious node in the presence of weakness

- receiver collision
- ambiguous collision,
- limited transmission power,
- partial dropping,
- false misbehavior report,
- collusion.

TWOACK [2] is to detect misbehaving links by acknowledging every data packet transmitted over each three consecutive nodes along the path from the source node to the destination node. Upon retrieval of a data packet from targeted mobile node, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. It has disadvantages such as unwanted network overhead due to two acknowledgements used in every data packet sent and degrade network performance.

S-ACK (Selective TWOACK) [2], a derivative of the TWOACK scheme, reduces this extra traffic due to TWOACK. In this, instead of sending back a TWOACK packet every time when a data packet is received, a node waits until a certain number of data packets (through the same triplet) arrive. It also suffers from network overhead.

Adaptive ACKnowledgment (AACK) [8] is a combination of an Enhanced-TWOACK(E-TWOACK), which detects misbehaving node instead of misbehaving link and an end-to end acknowledgment scheme, to reduce the routing overhead caused by TWOACK. It can't detect false misbehavior report and forge acknowledgement packets which made malicious node cause packet drop in network.

EAACK (Enhance Adaptive ACKnowledgement**)** [4] is to overcome three weakness of watchdog scheme such as false misbehavior report, limited transmission power and receiver collision.

It also solves forged acknowledgement and false misbehavior report in the above acknowledgement schemes. It consists of three parts (i) Acknowledge (ACK) (ii) Secure-ACKnowledgement (S-ACK) (iii) Misbehavior Report Authentication (MRA). ACK and S-ACK could not able to detect malicious nodes, if false misbehavior report is used by malicious node.

With MRA scheme, MANET can find alternative route to reach destination node due to its dynamic topology. EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report and it is achieved by use of ACK schemes. Acknowledgement should be digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet.

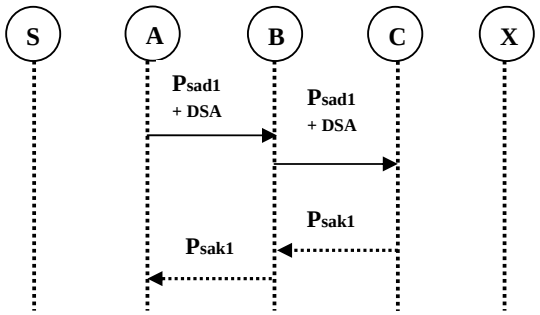

Fig 1: Enhanced Adaptive ACKnowledgement Scheme (EAACK)

Network performance is affected by routing overhead, due to use of both acknowledgement packets and digital signatures.

It is solved by using:

- Use an hybrid key management scheme to reduce the network overhead caused by digital signature.

- Adopt a key exchange mechanism to eliminate the requirement of pre distributed keys.

VI. Proposed Hybrid Cryptography Technique

Network overhead increases when number of malicious node in that network increases, because the count of acknowledged packet increases. Thus to reduce network overhead Hybrid key cryptography technique is used.

The proposed system uses Energy Efficient Dynamic Key (EEDK) consist of both Diffie Hellman key and RSA key pairs to be sent with the data packets [14] sent to destination node.

Diffie-Hellman algorithm is used as a form of authentication such as issue trust authority (TA) certificates by a TA server to ensure that symmetric keys are established between legitimate node. The data packet send from source node to destination on network through a base station such as Trust authority (TA) center. Packet drop is reduced by implementing the secret key generated for each mobile node in the network.

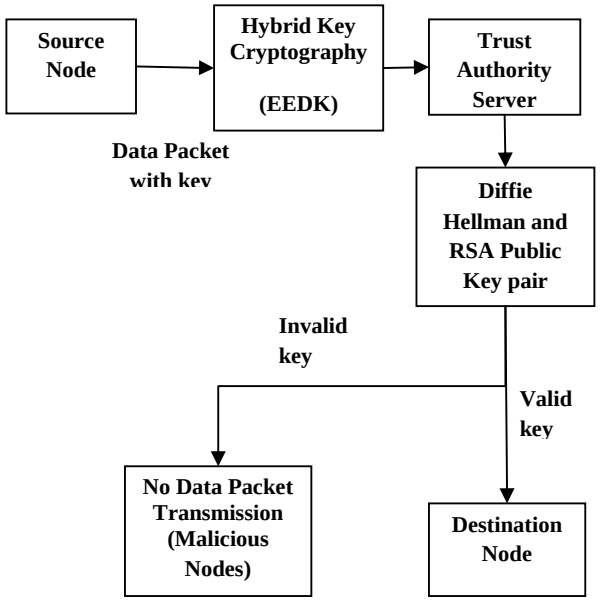

Fig 2: Hybrid Key Cryptography

RSA algorithm is used to generate public key and private key. The public and private key is different for all nodes in the entire network. Public key is used for encryption and Private key is used for Decryption. Source node send request to receiver after receiving the request destination node send the request to trust authority (TA) server with the secret message.

VII. Conclusion

Detection of Packet drop is always threat to security in MANETs and it uses several acknowledgement schemes such as TWOACK, S-ACK, AACK and EAACK to overcome the defect. Thus, EAACK out performances all other schemes and still suffer from higher Routing Overhead (RO) due to use of digital signature. In this paper, it gives hybrid key cryptography technique to overcome Routing Overhead (RO) by deleting malicious node's route. Source node and destination node both authenticate with a shared key to transfer data packets between them. Thus, Hybrid key cryptography scheme avoid routing overhead by deleting malicious node's route in MANET.

References

[1] A. Patcha and A. Mishra, "Collaborative Security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.

[2] Balakrishnan, K.,Jing Deng, Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks", InProceedings of Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137-2142(March 2005)

[3] E Surya et al, "A Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science & Communication Networks, Vol 2(4), 475-477, 2012.

[4] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, " EAACK-A Secure Intrusion-Detection System for MANETs",IEEE Transactions on industrial electronics, VOL. 60, NO. 3, March 2013.

[5] Feng He, Kuan Hao, and Hao Ma "S-MAODV:A Trust Key Computing Based Secure Multicast Ad-hoc On Demand Vector Routing Protocol" 2010 IEEE.

[6] Gaganpreet Kaur, Manjeet Singh, "Packet Monitor Scheme for Prevention of Black-hole Attack in Mobile Ad-hoc Network", JCSCE, NCRAET-2013.

[7] G.S Mamatha , Dr.S.C. Sharma "A Highly Secured approach against attacks in MANETS" IJCTE Vol.2, No.5, Oct 2010.

[8] 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.

[9] Mohan Kumar S B, Nirmal Kumar S Benni, "Cryptographic Approach to Overcome Black Hole Attack in MANETs",IJIET.

[10] P.Chaitanya and Y.Raja Sree, "Design of new security using symmetric and asymmetric cryptography algorithms", World Journal of Science and Technology 2(10):83-88, 2012.

[11] Pavithra Loganathan and Dr.T.Purushotaman, "An Energy Efficient Key Management and Authentication Technique for Multicasting in Adhoc Networks", JATIT, vol. 53, July 2013.

[12] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems" Commun.ACM, vol. 21, no. 2,pp. 120–126, Feb.1983.

[13] Ramandeep Kaur and Jaswinder Singh, "Towards Security against Malicious Node Attack in Mobile Ad Hoc Network", IJARCSSE, vol.3, July 2013.

[14] Amudha Bharathi.B, Dr.S.Usha, "Fortify Manets From Invasion Using Hybrid Cryptographic Techniques", IRACST,vol 3,Oct 2013.

[15] Venkatesan Balakrishnan and Vijay Varadharajan, "Packet Drop Attack: A Serious Threat To Operational Mobile Ad Hoc Networks".