RESEARCH ARTICLE OPEN ACCESS

Secure Hybrid Key Scheme to Detect Malicious Nodes in Manets

Anand .T *, Vedhavarshini .R**
*(Associate Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, India)
** (Master of Computer Science and Engineering, K.S.R.College of Engineering, Tiruchengode, India)

Abstract
Mobile Ad hoc NETwork (MANET) is a collection of independent mobile nodes that communicate with each other through wireless links without any centralized infrastructure. Nodes in MANET can act as hosts or routers to forward data packets to other mobile nodes in the wireless network. Nodes perform single hop network to forward data packets, if transmission range is within the limit. Nodes perform multihop network for data packets forward via intermediate nodes, if transmission range is beyond the limit. The Open medium and wide distribution of MANET make it vulnerable to various malicious attackers to degrade network performance. The Existing Intrusion Detection System (IDS) detect malicious nodes, but their routing overhead is high due to use of both acknowledgement packets and digital signatures. This paper gives solution to avoid high routing overhead by adopting a Hybrid key management scheme.
Keywords: IDS, Hybrid Key Scheme , MANET, Packet Drop Attack, Security

I. Introduction

A Mobile Ad hoc Network is a collection of wireless mobile nodes that are capable of communicate with every other nodes without any fixed infrastructure. It does not have any centralized administration and it is deployed in applications such as search and rescue, battle fields and disaster recovery. Mobile nodes can act as both transmitter and receiver to forward data packets between them through routing protocols [1] such as proactive (Eg: Destination Sequence Distance Vector), Reactive (Eg: Dynamic Source Routing, Adhoc On Demand Vector) and Hybrid (Eg: Zone Routing Protocol) routing protoclos.

The Characteristics of MANET are:

- Dynamic topologies
- Bandwidth-constrained links
- Energy constrained operation
- Limited physical security.

Routing protocols are often very vulnerable to node misbehavior. A node dropping all the packets is considered as malicious node or selfish nodes. A malicious node misbehaves because it cause damage to network functioning. Selfish node wants to save battery life for its own communication by simply not participating in the routing protocol or by not executing packet forwarding and Malicious node [2] is to falsely advertise very shortest routes and convince other mobile nodes to route their messages via that malicious node. The Intrusion Detection System act as second layer of defense against these malicious node in MANETs.

Security in MANET is important for basic functionality of entire network. It suffers from security attacks because of its feature like open medium, change its topology dynamically and lack of central management.

II. Security in MANET

Security requirements in MANET:

2.1. Availability

Ensures that network security services are available to the required parties when required.

2.2. Confidentiality

Ensures that the intended receivers can only access transmitted data. It is always provided by encryption.

2.3. Authenticity

Both sender and receiver of data need to be sure of each other's identity.

2.4. Integrity

Ensures that data has not been altered during transmission.

2.5 Non-Repudiation

Ensures that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data.

III. MANET Security Attacks

Due to multihop nature of Manets, it depends on cooperation among other nodes in the network. Cooperation between two nodes is required for efficient transfer of data packets between them. It undergoes several security challenges such as:

3.1. Internal Attacks

Internal attacks occur on nodes in network and link layer interface. This attack creates wrong routing information to other nodes. It is done by malicious nodes and difficult to identify compared to external attacks.

3.2. External Attacks

External attacks cause congestion in network. It leads to communication and additional overhead in network. Denial of Service (DoS) is a type of external attack.

3.3. Passive Attacks

In Passive attack, transmitted data does not altered in the network. But, it accumulates routing information by perform "unauthorized" listening to the network and affects network traffic.

3.4. Active Attacks

In Active attack, flow of message between nodes is prevented. It is done by either internal or external sources. Active internal attacks are caused by malicious or compromised nodes in internal network. DoS, Congestion traffic are example of active attacks. An active attack is classified as follows:

3.4.1. Dropping Attacks

Dropping attacks is caused by selfish nodes or compromised nodes in the network, by dropping all data packets. It prevents end to end communication between nodes.

3.4.2. Modification Attacks

It modifies all data packets in network and disrupts entire communication between them. Malicious nodes advertise itself having shortest route to reach destination, by modifying route information and data packets.

3.4.3. Fabrication Attacks

In Fabrication attack, fake route messages are send to nearby nodes in response to legitimate route request messages.

3.4.4. Timing Attacks

Attackers attack neighbour nodes by advertise itself a closer node to actual node.

IV. Attacks in Network Layer

In adhoc network, routing mechanism has three layers namely Network, Physical and MAC layers. Modifying some parameters of routing messages and selective forwarding attacks are attacks [3] in network layer. They are denoted as Gray hole attack and Black hole attack [4].

4.1. Gray hole attack

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node.

4.2. Black hole Attack

It is a type of denial of service attack in which malicious node attract all packets by giving a shortest route to reach the destination and intercept all the data packets in that [5] process. It leads to packet drop attack.

It affects end-to-end delay, throughput, network load, packet loss in the network and it degrade the network performance.

V. Packet Drop Attack

A Packet may be dropped [6] due to following reasons such as:

5.1 Unsteadiness of Medium

Packet may be dropped due to corruption and broken links

5.2. Geneuiness of node

Packet may be dropped due to overflow of transmission queue and lack of energy resources.

5.3. Selfishness of node

Packet may be dropped due to saving of its own energy resources.

5.4. Maliciousness of node

Packet is dropped due to malignant act of a node.

VI. Intrusion Detection in Manet

Intrusion Detection System (IDS) [7] is used to detect malicious nodes and to avoid packet drop in MANET. An IDS should be cooperative and energy efficient for 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 should utilize minimize resources to provide security to the mobile nodes.
- IDS must detect intrusion on each node and have run-time efficiency.

VII. Methods To Detect Intrusion in MANETS

Watchdog and Pathrater [8] form the basis for many of 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 these nodes. 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 [9] is to detect misbehaving links by acknowledging every data packet transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a data packet, 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 acknowledgement required by every data packet sent and it degrade network performance.

S-ACK (Selective TWOACK) [9], 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. The node then sends back one TWOACK packet acknowledging multiple data packets that have been received so far. It also suffers from network overhead.

Adaptive ACKnowledgement (AACK) [10] 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 of TWOACK. It can't detect false misbehavior report and forge acknowledgement packets.

EAACK(Enhanced Adaptive ACKnowledgement) [11] 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. Acknowledgement should be digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet.

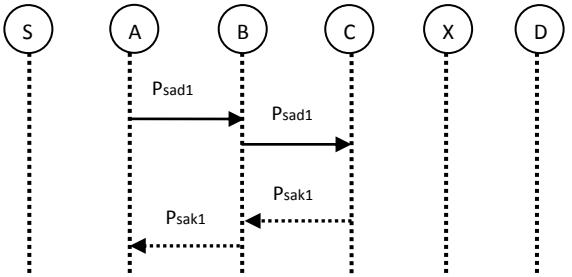

Fig 1: EAACK Scheme

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

It is solved by using Use a hybrid key management scheme to further reduce the network overhead caused by digital signature.
Adopt a key exchange mechanism to eliminate the requirement of pre distributed keys.

VIII. Hybrid Key Management Scheme

Hybrid key management is a mode of encryption that merges two or more encryption systems [12]. It incorporates a combination of asymmetric and symmetric encryption [13] to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security.

Whenever a source wants to transmit the data packets to the destination, it ensures that the source is communicating with real node. The authentication service uses a key management to retrieve the extended public key, which is trusted by the third party for identification of the destination. The destination also used similar method to authenticate the source. Through this, route with malicious node can't transmit their packets to the destination node.
In Energy Efficient Dynamic Key Management Scheme (EEDK) [14] , it uses both Diffie-hellman key pair and the RSA[15] secret public key pair to each of all the group members in the network. Here, the trust authority (TA) uses RSA secret public key pair and also establishes the public key certificates to each group member by signing public key with its secret key. It adopts a proactive secret share update algorithm. It also reduces routing overhead caused by use of Digital Signatures. Here, Source node and destination node both authenticate with a shared key to transfer data packets between them. Only a node with authenticated key can form a route to reach destination node. An alternative route with malicious node is deleted by use of this hybrid key scheme. Thus, it reduces routing overhead from existing system and also improves packet delivery ratio, network throughput of the system.

After execution of the key management module, a shared key is invoked. This is used by both source and destination for further communication confidentially. In this way, all the important data packets are transmitted to the destination with only minimum data packet loss.

IX. Conclusion

Detection of Packet dropping 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 overcome defects in all other schemes and still suffer from higher Routing Overhead (RO) due to use of digital signature and acknowledgement packets used between source node and destination node. In this paper, it gives hybrid key management scheme 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. Only a node with authenticated key can form a route to reach destination node. Thus, Hybrid key management scheme avoids routing overhead by deleting malicious node's route in MANET.

REFERENCES

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

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

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

[4] Tarunpreet Bhatia and A.K.Verma, "Security Issues in Manet : A Survey on Attacks and Defense Mechanisms" *IJARCSSE, vol. 3,* june 2013.

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

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

[7] Sunita Sahu and Shishir K. Shandilya**, "**A Comprehensive Survey On Intrusion Detection In Manet", *IJITKM, vol. 2, no.2*, pp. 305-310, Jul-Dec 2010.

[8] 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.

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

[10] 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.

[11] 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.

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

[13] 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.

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

[15] 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.