Secure Intrusion Detection System for MANETs Using Triple-DES Algorithm

Abhiram Shashank N[1, *], Bharathi C[2]

[1]Department of Computer science and engineering

[2]Saveetha School of Engineering, Saveetha University, Thandalam, India

Received 23 September 2017; received in revised form 30 November 2017; accepted 03 February 2018

Abstract

Networking is the process of accessing, exchanging or sharing the information. Packet switching plays a vital role in data transfer. Compared to wired network, wireless network has more data transferring. MANETs and WSN are the most common forms of Wireless media; in MANETs nodes are deployed or distributed in Ad-hoc way and they are communicating or exchange message using wireless Transmission. Security is a measure concern in Mobile Ad-hoc Network because MANETs have wide distribution of node and open medium; therefore, it becomes vulnerable and is easy for malicious hackers to attack.

Keywords: Mobile Adhoc Network (MANET), Intrusion Detection System (IDS)

1. Introduction

Networks are a group of system networks linking together. There are two main classifications, Peer to Peer and Client/Server. Networks can be characterized by their size and purpose. The size of the network is explained by geographical area that they occupy and the number of links that are part of the network. Some networks based on size are; LAN (Local Area Network), WAN (Wide Area Network), MAN (Metropolitan Area Network), PAN (Personal Area Network). Some Networks based on their purpose are; SAN (Storage Area Network), VPN (Virtual Private Network), MANET (Mobile Ad-Hoc Network). In this paper we discussed about the intrusion detection systems on MANETS.

Mobile Ad-Hoc Network or MANET is an infrastructure-less IP based on network of mobile and wireless machine nodes. It is a type of ad-hoc network that can change locations and configure itself while moving. In MANET each node act as a "router" to transmit the traffic to other specific node in the network.

MANETs is very successive, attractive, and pervasive technology in wireless network. To maintain the mobility is an important task done by Manets. MANETS is much more easier to be affected by different types of attack because it provides distributed architecture, volatile network topology, limited bandwidth of single hop and multi hope. In single hope, the entire node is in the defined coverage area, if there is intermediate node used for communication between two nodes is been called multi hop network. In MANETs there are two types of attack possible one is active attack and the other is Passive attack. MANETs is used in emergency requirements because it allows easy deployment, minimal configuration, and low cost. However, it has restricted the battery power and resources.

The aim of networking is to facilitate the exchange of data such as audio, text or video between various points across the world. For the delivery of data, various types of switching techniques are used in networking. The various types of switching techniques are packet switching, message switching and circuit switching. In this paper, we are dealt with packet switching.

* Corresponding author. E-mail address: abhiramsashank@gmail.com, cbharathi26@gmail.com

Packet switching is a method of transferring the data in a form of packets to a network. To transfer the information fast and efficient, the data are broken into small pieces of variable length, called Packet. The receiver has to reassemble these packets into a same file to retrieve the information. Each packet carries the information of source and destination address, using them to travel independently through the network. The packets belonging to same files may or may not travel through same path. There are two types of packet switching; Connection-Oriented Packet Switching (virtual circuit) and Connectionless Packet Switching (Datagram). In this paper, we are dealt with Connectionless Packet Switching (Datagram).

Each packets in the Datagram contains all necessary addressing information, such as source address, destination address and port numbers etc. In Datagram each packet acts independently. Packets that belong to same file may take different routes because of the dynamic routing technique; therefore, the packets arrived to destination are out of order. In Fig.1, the receiver send the packets to different transmission path and reach to different destination. In connectionless setup, packet delivery is not guaranteed; therefore, the receiver has to provide delivery acknowledgement using additional protocols and request for missing packets. Packet switching is cost beneficial because the devices do not need massive amount of secondary storage.

The delays in Packet switching are: Transmission Delay, Propagation Delay, Queuing Delay, and Processing Delay. Transmission delay is simply time required to put data bits on the wire/communication medium, and it depends on length of packet and bandwidth of network. Propagation delay is time taken by the first bit to travel from sender to receiver and it depends on distance and propagation speed. Queuing delay is time where a process waits in a queue until it can be executed. It is the time difference between the arrival of packet and the start of the data process. Processing delay is the time required to process the packet’s header and determine where to direct the packet.

2. Internet Attacks

Networks are often subjected to attack without any security measures, example-internet. There are two types of attacks;

- Active attack
- Passive attack

Active attack is a network attack that the intruder tries to alter the information on data that has being transferred. Passive attack is a network attack in which the information is not altered but monitored or overheard while transmission.

The both active and passive attacks are further classified.

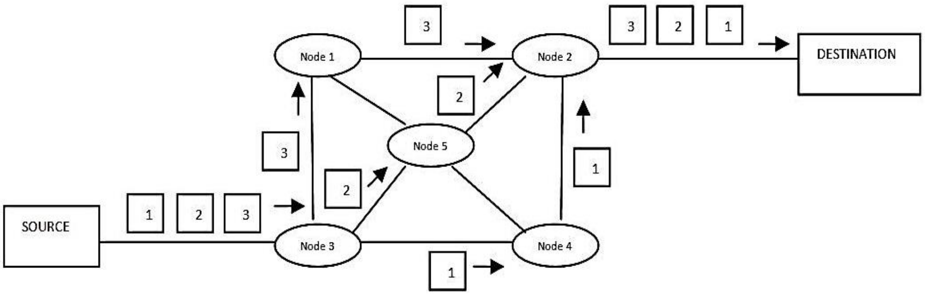

Fig. 1 Packet Switching – Connectionless (Datagram)

The types of active attacks:

- Masquerade
- Replay
- Denial of Service attack
- Modification of messages

The types of passive attacks:

- Traffic analysis
- Eavesdropping
- Man in the middle attack

2.1. Active attacks

2.1.1 Masquerade attack

It is an attack that uses fake identity. The attackers pretends to be an authorized user of a system to gain access to personal computer information, such as stolen Ids and passwords. If the authorization is not fully protected, then it became vulnerable to masquerade attack. Once the attackers entry, they have a full access. This attack occurs more in an organisation where they modify data or software, and may also alter the network configuration and routing information.

2.1.2 Replay attack

It is a network attack that the intruder detects data transmission and make the transmission maliciously delayed or repeated, i.e. a replay is an attack on security protocol that replays the data transmission from a sender to the intended receiver, so as to fool the participants to believe they successfully completed the transmission of data. The message is encrypted correctly so that the receiver mistake it as a correct request and does the actions provided by the intruder.

2.1.3 Denial of service attack

It is a type of cyber attack which the intruder makes the network resource temporarily or indefinitely unavailable the user's service or indefinitely disrupting service. It prevents the users from accessing the specified computer systems or networks. Denial of service attack floods the servers with traffic, in order to make it difficult for the users to connect them. Attackers mostly attack web servers of high-profile organisations. DoS attacks do not led to the loss of information, but the the users have to deal with money and time complexity.

2.1.4 Modification of messages

It is an attack which the intruder alters packet header address, to direct the packets to different destination intended by the intruder or change the data and send them to to the targeted machine. This also includes deletion of data, alteration or insertion in an unauthorized manner.

2.2. Passive attacks

2.2.1 Traffic analysis attack

It is a type of attack against encryption. The common way to secure the contents is encryption. The intruders could observe the traffic patterns of these messages. The attackers' posses some basic information about network, i.e. the activity of the network, protocol being used and also access points of the network. The attackers can determine the location, the host and also the frequency and length of messages being exchanged. Traffic analysis can determine what type of data is being communicated even if the data is scrambled or encrypted. The size of packets being exchanged between two hosts can also be valuable information for an attacker, even if the contents can't be viewed. Traffic analysis is very difficult to detect because they do not involve any change in the data.

2.2.2 Eavesdropping attack

Real-time interception of private communication is unauthorized, i.e. phone call, instant message, fax, video call. It also weakened between client and server that allows intruder to send traffic to it. This type of network attack is due to lack of encryption services. Attackers can install network monitoring software on a computer to carryout eavesdropping and intercept data. Using firewalls, antivirus software, and virtual private networks and avoid sending sensitive information on public networks prevent eavesdropping attacks.

2.2.3 Eavesdropping attack

It is a type of cyber attack which the intrudergains information on data between two parties by eavesdropping or impersonating. MitM attack is a serious threat to online security because the attacker have is able to capture and manipulate sensitive information in real-time. MitM attacks distributes malware that provides the attackers access user's web browser and data that are exchanged. Online banking and e-commerce are sites that MitM attackers target.

3. Acknowledgment Schemas

There are numerous IDS (Intrusion Detection System) produced for giving security. The various approaches to find IDS are,

3.1. ACK (Acknowledgement) schema

In this schema, the receiver sends an ACK in form of signal to the sender as a receipt that the data is transmitted to destination successfully. The ACK is received after the transmission of every data block. The sender sends the next block of data only after it receives ACK from previous block of data. It is an indication that the data been transmitted has been received uncorrupted and there's no errors of receiving station.

3.2. NACK (Negative Acknowledgement) schema

In this schema, the sender receives N-ACK or REJ (rejection) when the file received by the receiver is corrupted. An alternate signal ARQ (Automatic Request for retransmission) is automatically generated when there is N-ACK. When source receives NAK or REJ signal from the destination, the source either re-transmits the data or stops the transmission process entirely.

3.3. WATCHDOG schema

This schema detects the malicious node which is unsafe to establish connection. It is has two operations: phase1-watchog, phase2-pathrater. Watchdog uses next hops transmission for detecting malicious attack. However, it increases the failure if the next node fails to establish transmission within intended time interval. Pathrater make sure the malicious node been detected by watchdog is not been used later or for future purpose.

3.4. TWOACK schema

In this schema, the TWOACK uses three consecutive nodes to check whether the packet is transmitted successfully. It is achieved by acknowledging the data over every three consecutive nodes. In other hand, MANETs allows the node to self organize for functioning, the performing nodes consumes energy and other resources. Therefore, the network nodes may decide to be non co-operative with other nodes to perform well individually which affects other nodes. This kind of nodes is said to be selfish nodes or misbehaving nodes. The schema makes sure that nodes are not used later or future purpose.

3.5. AACK (Adaptive Acknowledgement) schema

This schema is the combination of TWOACK and ACK. It has end-end transmission. Source sends the packets through nodes to the destination. Once received, the receiver sends an ACK in the reverse order. This process should be done within predefined interval; if not, then it will switch to TWOACK process.

4. Cryptography Algorithms

Cryptography algorithms can be fundamentally divided into

- Symmetric
- Asymmetric
- Hash functions

In this paper we are dealing with symmetric algorithms.

4.1. Symmetric Algorithm

Symmetric algorithm encrypts and decrypts a data using the same key. Anybody who holds a key can exchange message with anybody else holding the same key. Once intruder get the key, they can access the message; therefore, the key must be shared secretly. The most commonly used symmetric algorithm is DES.

4.4.1. Data Encryption Standard (DES)

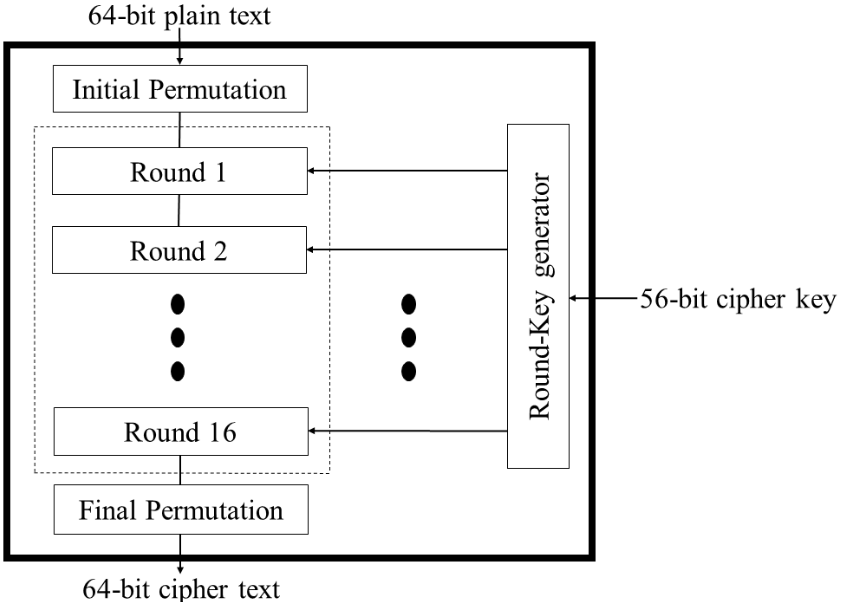

Fig. 2 Data Encryption Standard

It is a symmetric-key block cipher. It is an implementation of a feistel cipher. The block size is 64-bit but the key length is 56 bits, since 8 of the 64 bits key is not used by the encryption algorithm as shown in Fig. 2.

The process or steps involved in fiestal cipher are:

- Round Function
- Key Generation

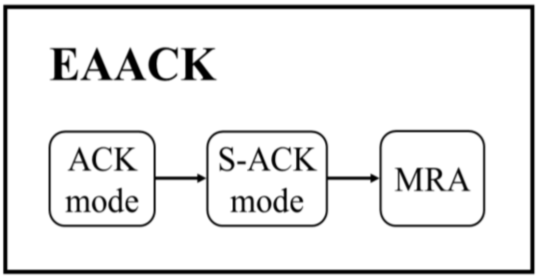

Fig. 3 Enhanced Adaptive Acknowledgement (EAACK)

Round function: the cipher follows DES function. The DES function applies 48-bits key to the rightmost 32-bits to produce a 32-bit output. In round function P-boxes and S-boxes are used, also known as Initial and Final Permutation.

Permutation-box (P-box) is a method of bit-shuffling used to transpose bits across S-boxes inputs. P-boxes are used for expansion, compression and straight accordingly with respect to number of output bits that is less than, greater than or equal to the number of input bits.

Substitution-box (S-box) is a vital component of symmetric key algorithms which performs substitution. S-box takes m number of inputs and transforms them into n number of outputs, where n is not necessarily equal to m.

Key generation: DES input key size is 64 which contain 56 bit key and 8 bit parity. Parity bits are 8th bit of every 8 bit (one byte). Therefore, they are the multiple of eight: 8, 16, 24, 32, 40, 48, 56 and 64. Permuted Choice PC-1 is used to remove these bits from the 64 bit input key. So PC-1 gives 56 bits as output.

5. MECHANISM

The mechanisms used in this paper are

- EAACK
- HYBRID CRYPTOGRAPHY
- TRIPLE DES ALGORITHM

5.1. EAACK

- Acknowledgement (ACK)
- S-Acknowledgement (S-ACK)
- Misbehaviour Report Authentication (MRA)

5.1.1 Acknowledgement (ACK)

Refer to Fig.3. Here the ACK schema acts as a part of the hybrid scheme in EAACK to reduce network overhead.

5.1.2 S-Acknowledgement (S-ACK)

In this acknowledgement schema, the receiver can inform the sender about all segments of data that has been received successfully. The sender understands the drop of packets when the particular segment is not acknowledged. Thus the sender only needs to re-transmit the segments that has been lost.

5.1.3 Misbehavior Report Authentication (MRA)

This schema is able to detect malicious nodes which produce false misbehavior report. False behavior report is generated by intruders when they break down some nodes and divert the network. MRA verify whether the report on false misbehavior is received by different node. When the destination node receives MRA packet, it searches through its local knowledge base and compare whether the report packet is received by another node. If so, then it is understood that this false misbehaviour report and node is marked malicious.

5.2. Hybrid cryptography

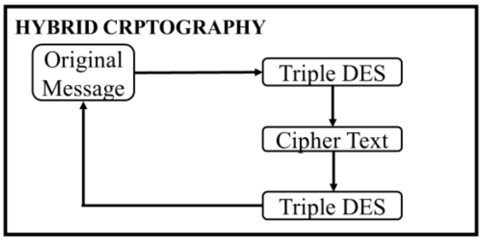

Fig. 4 Hybrid Cryptography

A hybrid cryptosystem is the one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. In this project, we used Triple DES Algorithm as a symmetric-key cipher, which applies the DES cipher algorithm three times to each data block as shown in Fig. 4. It is very easy to modify the existing software to use Triple DES. There is also the advantage of reliability and longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

5.2.1 Triple DES Algorithm

Triple DES is based on the DES (Data Encryption Standard) algorithm. DES has proven reliability and a longer key length to prevent many of the internet attacks. However even this algorithm is not strong enough to secure the data very long. Thus Triple DES was endorsed as a replacement for DES. The Triple DES uses the key of size 56 which runs the algorithm in succession with three different keys. The result of the key size will be 168 bits.

The Triple DES follows encryption-decryption process as follows

- Encrypt the plaintext using Single DES-Key K1
- Then decrypt the output of step 1 using Single DES-Key K2
- Finally encrypt the output of step 2 using single DES-Key K3
- The final result is the Cipher text
- Decryption process is just reverse of encryption process

5.3. Benefits

- EAACK gives better performance than other schema.
- EAACK uses digital signature it causes routing overhead.
- Hybrid cryptography is used to reduce routing overhead by detecting malicious path. Using shared key source node and destination node authenticate to transfer data Packet.

6. Conclusions

IDS (Intrusion Detection System) is important for providing security to MANETs it use acknowledgment schema such as TWOACK, ACK, AACK, EAACK to avoid the defect. EAACK gives better performance than other schema. EAACK uses digital signature and causes routing overhead. Therefore, this paper proposes techniques to reduce routing overhead by detecting malicious path. Using shared key source node and destination node transfer data Packet.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] P. Joshi, P. Nande, A. Pawar, P. Shinde, and R. Umbrae, “Eaack- secure intrusion detection and prevention system for mantes,” in Pervasive Computing (ICPC), International Conference on, January 2015.

[2] S. S. Jathe, V. Dhamdhere “Hybrid cryptography for secure superior malicious behavior detection and prevention system for MANET’s,” International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297:2007 Certified Organization) vol. 4, July 2015.

[3] R. Meher, S. Ladhe “Review paper on flooding attack in MANET,” Ruchita Meher et al Int. Journal of Engineering Research and Applications, vol. 4, pp. 39-46, January 2014.

[4] P. D. Nikam, V. Raut “Attacks prevention and detection techniques in MANET: a survey,” Pranjali D. Nikam Int. Journal of Engineering Research and Applications, vol. 4, pp. 15-19, November 2014.

[5] B. Suruthi, N. V. R. Kumar, and M. Tech. “An enhanced intrusion detection system for MANETs using hybrid key cryptography,” vol. 5, 2014.

[6] A. P. Tapaswi, P. P. Nashikkar, R. S. Barge, A. M. Shinde, and P. P. Patil “Extended EAACK an secure intrusion detection system with detection and localization of multiple spoofing attackers in MANET,” vol. 4, pp. 39-46, January 2014.

[7] H. Khatri, A. Gupta, and D. Pal “Mitigation of HTTP-GET flood Attack” International Journal for Research in Applied Science & Engineering,” vol. 2 November 2014.

[8] Ramya K, Beaulah David and Shaheen H, “Hybrid cryptography algorithms for enhanced adaptive acknowledgement secure in MANET,” vol. 16, February 2014.

[9] E. M. Shakshuki, N. Kang, and T. R. Sheltami, “EAACK a secure intrusion-detection system for MANETs,” IEEE Transactions On Industrial Electronics, vol. 60, March 2013.

[10] S. M. Lakshmi, S. Bhavana, T. Sujata, “Enhancement of security levels using a secure intrusion detection system in manets,” K. Anusha, and G.V. Rajyalakshmi,” Secure Adaptive Acknowledgement Algorithm for Intrusion Detection System” Int, vol. 16, May 2014.

[11] B. Thanikaivel, B. Pranisa, Department of Computer Science and Engineering, Sona College of Technology Salem, Tamil Nadu, India, “Fast and secure data transmission in MANET,” 2012 International Conference on Computer Communication and Informatics (ICCCI - 2012), Coimbatore, India, January 2012.

[12] D. Sandhiya, K. Sangeetha, R. S. Latha, “Adaptive acknowledgement technique with key exchange mechanism for MANET,” 2012.

[13] N. Kang, E. Shakshuki, and T. R. Sheltami, “Detecting forged acknowledgements in MANETs,” in Proc. IEEE 25th Int. Conf.AINA, Biopolis, Singapore, pp. 488-494, March 2011.

[14] R. Ferdous, V. Muthukkumarasamy, and A. Sattar, Institute for Integrated and Intelligent Systems Griffith University, Australia, “Trust management scheme for mobile Ad-Hoc Networks” 10th IEEE International Conference on Computer and Information Technology, 2010.

[15] B. Pahlevanzadeh, S. A. Hosseini Seno, T. C. Wan, R. Buldiarto, and M. M. Kadhum, “A cluster based distributed hierarchical IDS for MANETs,” International Conference on Network Applications, Protocols and Services, pp. 1-7, November 2008.

[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs,” IEEE Trans. Mobile Computer, vol. 6, pp. 536-550, May 2007.

[17] B. Pahlevanzadeh, and A. Samsudin, “Distributed hierarchical IDS for MANET over AODV” IEEE International Conference on Telecommunications and Communications, pp. 99-104, May 2007.

[18] G. Jayakumar and G. Gopinath, “Ad hoc mobile wireless networks routing protocol-a review,” J. Comput. Sci., vol. 3, no. 8, pp. 574-582, 2007.

[19] S. Marti, T. J. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in Ad-hoc Networks,” pp. 255-265, 2000.

[20] T. Anantvalee and J. Wu, “A survey on intrusion detection in mobile Ad Hoc Networks,” in Wireless/Mobile Security, New York, 2006.