EFFECTIVE DATA EXCHANGE MECHANISM FOR MANETS USING DIFFIE HELLMAN KEY EXCHANGE ALGORITHM

Kanusu Srinivas Rao[1], Ratna Kumara Challa[2], M.Sridhar[3]

[1]*Dept. of Computer Applications, Yogi Vemana University Kadapa, Andhra Pradesh, (India)*

[2]*Dept. of Computer Science & Engg, JNTUK, Kakinada, Andhra Pradesh, (India)*

[3]*Dept. of Computer Applications, R.V.R & J.C College of Engg, Andhra Pradesh, (India)*

ABSTRACT

Mobile Ad-hoc networks are very sensitive to security threats due to their nature of deployment such as open wireless medium. It gives chances to various types of attacks. Existing system with stand the packet dropping attack using EAACK protocol specifically designed for MANETs. It also focused on initiating forged acknowledgement attacks and applied digital signatures as a preventive or detection measure for such type of attacks.The limitation of existing system (EAACK) protocol is network overhead due to Digital Signatures as well as static key exchange mechanism. It will some time lead to security threats in case of node compromise.To overcome the above problems, proposed system introducing dynamic or adaptive key exchange mechanism. The advantage of this mechanism is, adaptively or based on the requirement new keys are derived and exchanged among nodes. Due to this mechanism data transformation between mobile nodes are done with improved or high security. Storage overhead will be reduced because there is no need to maintain all other node keys at each node.

Keywords: MANETs, Diffie Hellman Key Exchange, EAACK, Digital Signatures.

I. INTRODUCTION

Networks have become a part of our life style due to their services. Networking is the process of communication or sharing information between two or more devices. There are two types of networks.

1) Wired networks.2) Wireless network.

Wired networks are networks which have physical connection between devices. Wireless network doesn't have any physical connection among devices.

The Mobile Ad-Hoc Network is the best example for a wireless network. The MANET is an infrastructure less,self-organizing and self configuring network of mobile nodes. MANET is a collection of mobile nodes. It does not have fixed routers. All nodes are capable of either sending or receiving the data. When two nodes are reside samecommunication range,they communicate directly with each other. Otherwise, they rely on their neighbours to transmit messages.

The ability of self-configuring nodes in MANET made it popular among critical mission applications like military applications or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is very important and necessary to develop efficient intrusion-detection mechanisms to protect MANET from attacks.

The basic philosophy behind MANETs is that, while the capability of each individual mobile node is limited, the aggregate power of the entire network is sufficient for the required mission.

II. LITERATURE SURVEY

Intrusion detection is the process of identifying the actions which are going to compromise the integrity, confidentiality, and availability of a resource i.e. nothing but the security verification. Intrusion detection systems should be added to enhance and improve the level of the security in MANETs.

2.1 Intrusion detection system (IDS) models

2.1.1 Watchdog:

The Watchdog scheme consists of two parts, namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network. It generates reports on misbehaving nodes. The Pathrater cooperates with the routing protocols inorder to avoid the reported nodes in the future transmission.

The Watchdog scheme fails to detect malicious misbehaviours with the presence of the following:

- Ambiguous collisions
- Receiver collisions
- Limited transmission power
- Falsemisbehaviour report
- Collusion and
- Partial dropping

2.1.2 Twoack

TWOACK detects misbehaving links in the path from the source to the destination by acknowledging every data packet transmitted over every three consecutive nodes. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. The process of acknowledging in every packet transmission is required andadded a significant amount of unwanted network overhead. Due to the limited capacity of battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

2.1.3 AACK

Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called Acknowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still have the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgment packets.

2.2 EAACK

Elhadi.M.Shakshuki, Nan keng and tarek.R.sheltami proposed a new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK). EAACK which contains three parts ACK, Secure ACK (SACK) and misbehaviour report authentication. All the parts of EAACK (ACK, S-ACK, MRA) are acknowledgement based detection systems. In this approach acknowledgement packets play a vital role to identify misbehaviours in the net-work.

i) ACK

ACK is an acknowledgement scheme in which acknowledgement packet travel from end to end. If the packet is not send back to source, then misbehaviour is identified.

ii) **S-ACK**:

S-ACK mode is to detect misbehavior nodes in the presence of receiver collision or limited transmission power. In the S-ACK, the main principle is to let every three consecutive nodes work in a group to detect misbehaving nodes.

iii) **MRA**:

The Miss-behavior Report Authentication resolves the problem in watchdog with respect to the false misbehavior report.

In EAACK based approach, to provide more authenticity to the acknowledgement packets they incorporated digital signature scheme by implementing DSA.

III. PROPOSED SYSTEM

In MANETs source node and destination nodes are communicate with each other using acknowledgement packets for secure data transmission. The question of key exchange was one of the problems because attackers' have always kept their observation on network to decrypt the data in unauthorized way. For secure data transmission in MANETs we propose Diffie Hellman key exchange algorithm. As the communication channel is insecure, it provides security without sharing their private keys. So there is no chance to the intruder to get the knowledge about private keys of source node and destination node.

Diffie-Hellman algorithm:

Nodes should agree on a key that two nodes can use for a symmetric encryption

Step1:

Source node and destination nodes agree on a prime number **p** and a generator base **g**. (**g**<**p** and **g** a primitive root of **p**). These two values **p** and **g** can be publicly advertized.

Step2:

In this step source takes a private key **a**. And destination takes its own private key **a**, **b** values are secret keys which do not reveal to anyone.

Step3:

Source can compute the value for **X.**

$$X = ga\ (\mathrm{mod}\ p)$$

Destination can compute the values for **Y.**

$$Y=gb\ (\mathrm{mod}\ p)$$

Step4:

The values X and Y are exchanged between source and destination nodes. Since they sent over the insecure channel, the intruder or eavesdropper can hot identify secrete keys. So source can have a, Y, g, p and destination can have b, X, g, p;

At source machine shared key will be

$$\alpha = Ya\ (\mathrm{mod}\ p)$$

At destination machine share key will be

$$\beta= Xb\ (\mathrm{mod}\ p)$$

IV. CONCLUSION

In MANETs, intrusion detection systems are used to find malicious attacks, and nodes. It is not that easy to provide security for MANETs because of its special features. Here in this paper we proposed an effective data exchange mechanism for MANETs using Diffie Hellman key exchange algorithm. By using this scheme we can transmit data effectively as compared with the previous or existing techniques among nodes or devices in the network. This is a mechanism that works better even the communication channel is insecure.

REFERENCES

[1]. N. Kang, E. Shakshuki, and T. Sheltami, “Detecting misbehaving nodes in MANETs,” in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[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]. “An effective Diffie-hell man key based intrusion detection to secure for multicast routing in manet”, m.dhivyasri, P.G. Scholar Department of Information Technology, VCEW. P.E.Prem, assistant professor information technology VCEW, nithyasri, assistant professor information technlogy VCEW.

[4]. 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.

[5]. B. Sun, “Intrusion detection in mobile ad hoc networks,” Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[6]. Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[7]. R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

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

[9]. 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 Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[10]. 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.

[11]. L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[12]. "A study of different types of attacks on multicast in mobile ad hoc networks" Hoang Lan Nguyen, UyenTrang Nguyen, Elsevier AdHoc Networks(2008) 32-46.

[13]. 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.

[14]. B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[15]. Rohit Rawat "DEMAND SIDE MANAGEMENT BY SOLAR PHOTOVOLTAIC MODULE" International Journal of Electrical and Electronics Engineers, Vol.7 No. 2, -2321-2055, 2015.