ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

A Secure and Improved Intrusion discovery system for the vulnerable Mobile Ad-Hoc Networks

Golla Subramanyam
M.Tech Student ,
Computer Science Engineering Department,
Dr.K.V.Subba Reddy Institute Of Technology.

C.Md Gulzar
Associate Professor,
Computer Science Engineering Department,
Dr.K.V.Subba Reddy Institute Of Technology.

Abstract:

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes.

This results in a highly dynamic, autonomous topology. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller. The open medium allows MANET vulnerable to attacks. In existing system Enhanced Adaptive Acknowledgment(EAACK) method is imposed, in this digital signature method is used which cause network overhead. Thus proposed system specifies the Hybrid Cryptography technique isused to reduce network overhead.

Keywords:

Wirelss Networks, AD-HoC Netwrorks, Digital Signature, Enhanced Adaptive ACKnowledgment (EAACK). Nodes.

Introduction:

A MANET is a type of ad hoc network that can change locations and configure itself on the fly.

Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment.

While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.

In computing, a wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention). The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices.

These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure, although they may be deployed standalone to enforce no-wireless policies within an organization. Some advanced wireless infrastructure has integrated WIPS capabilities. A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Rogue devices can spoof MAC address of an authorized network device as their own. New research uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.

The following types of threats can be prevented by a good Intrusion detection and prevention system:

- Rogue AP – WIPS should understand the difference between Rogue AP and External (neighbor's) AP.
- Mis-configured AP.
- Client Mis-association.
- Unauthorized association.
- Man in the Middle Attack.
- Ad hoc Networks.
- MAC-Spoofing.
- Honeypot / Evil Twin Attack.
- Denial of Service (DoS) Attack.

The movement to wireless network from wired network has been a worldwide development in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most significant and distinctive applications.

On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; each single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications.

To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

RELATED WORK/BACKGROUND:

1.EAACK-A Secure Intrusion Detection System forMANETS, Elhadi M.Shakshuki, Nan Kang, TarekR.Sheltami, explains various IDS in MANET and its disadvantages, EAACK its support in solving false misbheaviour report problem.

2. A Survey on Intrusion Detection in Mobile Ad-hoc Networks in wireless/mobile security, T.Anantvalee J.Wu, provides survey of various Intrusion Detection implementation in mobile ad-hoc networks.

3.Ad-hoc mobile wireless networks routing protocol-A review, G.Jayakumar G.Gopinath, explains different routing protocols like reactive and proactive protocols and its importance in MANET.

4.Detecting misbehaving nodes in MANETS, N.Kang M.Shakshuki T.Sheltami, clarifies the methods in identifying malicious nodes caused by attacks, and someways to prevent the network from intruders.

5.Detecting Forged acknowledgments in MANETS, N.Kang E.Shakshuki, specifies the security is based on acknowledgement packets, how to safeguard those packets from attacks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

6.Enhanced intrusion detection system for discovering malicious nodes in mobile ad-hoc network, N.Nasser Y.Chen, provides an improved technique Enhanced Adaptive Acknowledgement for detecting malicious nodes in network.

7.A method of obtaining digital signatures and public-key cryptosystems, R.Rivest A.Shamir L.Adleman, significant ways of enveloping packets with digital signature and public-key cryptosystems.

8.Industrial wireless sensor networks: challenges, principles and technical approach, V.C.Gungor G.Hanke, provides the various applications of wireless networks in industries.

EXISTING SYSTEM:

By definition, Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks.

In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or noncooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

DISADVANTAGES OF EXISTING SYSTEM:

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

1) ambiguous collisions;

2) receiver collisions;

3) limited transmission power;

4) false misbehavior report;

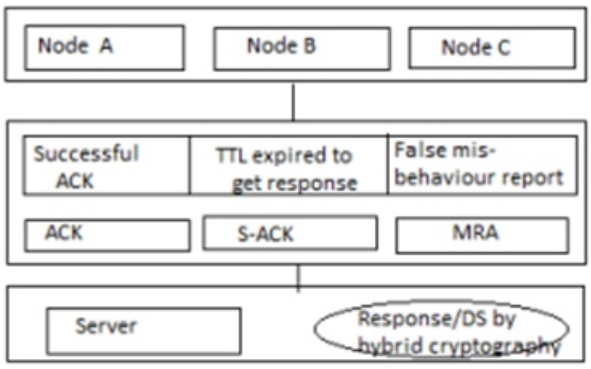
5) collusion; and

6) partial dropping.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

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

PROPOSED SYSTEM:



System Architecture

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

ADVANTAGES OF PROPOSED SYSTEM:

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision.

CONCLUSION AND FUTURE WORK:

The newly proposed scheme called EAACK, and it provides better performances comparing to all other existing approaches. The EAACK scheme implements digital signature which causes network overhead which can befurther reduced by hybrid key cryptography.

This cryptography technique uses RSA, AES for providing security and Zone Routing Protocol (ZRP) to find the route between source and destination. To allow the execution of EAACK scheme in real time environment to obtain accurate results for testing.

REFERENCES:

[1].Elhadi M. Shakshuki, Senior member, IEEE, Nan Kang, and Tarek R.Sheltami, IEEE; EAACK – A Secure Intrusion Detection System for MANETS; IEEE Transactions on Industrial Electronics, vol.60,No.3, March 2013.

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

[3]. William Stallings, Cryptography and Network Security, Fourth Edition,June 3, 2010.

[4]. G. Jayakumar, G.Gopinath, Ad hoc mobile wireless networks routing protocol-A review, vol. 3, No. 8, pp. 574-582, 2007.

[5]. T.Anantvalee and J.Wu, A Survey on Intrusion Detection in Mobile Adhoc Networks, NewYork: Springer 2008.

[6]. Minimized Routing Protocol in Ad-hoc Network with Quality Maintenance Based on Genetic Algorithm: A Survey, Upasna, Jyoti chauhan, Manisha, IJSRP, vol. 3, Issue 1, January 2013.

[7]. R.H.Akbani, S.Patel and D.C.Jinwala, DOS attacks in mobile adhoc networks, A Survey in proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012,pp.535-541.

[8]. A Secure data transmission in MANETS using Hybrid Scheme, Sowmya Thomas, Syam Gopi, IJERT,Vol. 2, Issue 8,August 2013.

[9]. Dr.E. Ramaraj, S. karthikeyan, M.Hemalatha, A Design of Security Protocol Using Hybrid Encryption Technique(AES-Rijndael and RSA) International Journal of the Computer, the Internet and Management, Vol.17, No.1,(January-April 2009)pp 78-86.

[10]. Y.Hu.D.Johnson, and A.Perrig, and D.Johnson, ARIADNE: A Secure on-demand routing protocol for ad -hoc networks, pp. 3-13.

[11]. Hybrid cryptography by the implementation of RSA and AES, Palaniswamy. V, Jeneba Mary, International Journal of Current Research, Vol. 33, Issue 4, pp. 241-244,april 2011.

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

[13]. N.Kang, E.Shakshuki, and Sheltami, Detecting misbehaving nodes in MANETS, in Proc. 12th Int. Conf. IIWAS, Nov.2010, pp.216-222.

[14]. 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 Computing, vol. 6,no.5, pp. 536-550.

[15]. N.Nasser and Y.Chen, Enhanced Intrusion Detection systems for discovering malicious nodes in mobile ad hoc networks, in Proc. IEEE Int. Conf. Commun, Glasgow, Scotland, June 2007, pp.1154-1159.