International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Using 3GPP- A Secure IDS for MANETs

Monika Garg, Karanvir Kaur, Simerpreet Kaur
Computer Science, Lovely Professional University, Phagwara, Punjab
monikagarg.lpu@gmail.com
Computer Science, Lovely Professional University, Phagwara, Punjab
simerpreet3@gmail.com
Computer Science, Lovely Professional University, Phagwara, Punjab
karanvir.14856@lpu.co.in

ABSTRACT

Mobile Ad hoc NETwork (MANET) is one of the important and unique applications. MANET does not require a fixed network infrastructure, every 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 else they can propagate message to neighbor nodes to pass the message. A new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report. The results will demonstrate positive performances against Watchdog, TWOACK and AACK in the cases of receiver collision, limited transmission power and false misbehavior report. EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances. EAACK is designed based on the Digital signature Algorithm (DSA) and RSA. Those techniques have drawback due to network overhead. We need techniques for security like encryptions, hybrid encryption or sign encryption to protect our message.

General Terms

Digital Signature Algorithm, 3GPP Algorithm (f8 and f9)

Indexing terms

MANET, IDS, EAACK, Digital signature, DSR, AODV, 3GPP

INTRODUCTION

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. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. They can be used in scenarios in which no infrastructure exists, or in which the existing infrastructure does not meet application requirements for reasons such as security or cost. Applications such as military exercises, disaster relief, and mine site operation may benefit from ad hoc networking, but secure and reliable communication is a necessary prerequisite for such applications. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own.

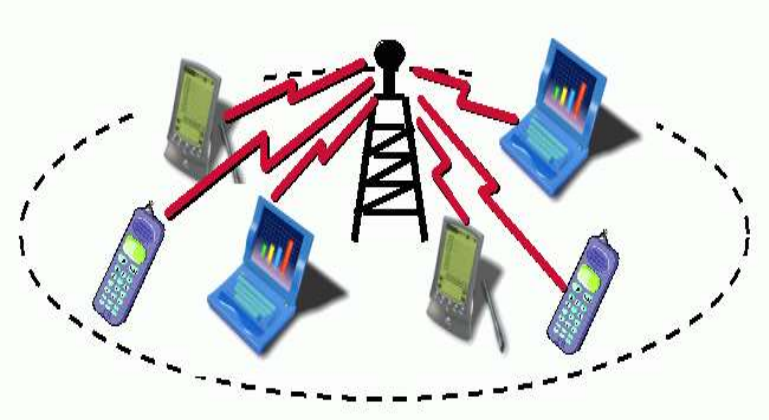

Fig. 1 Mobile Ad Hoc Network

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

FEATURES AND CHALLANGES

Features like autonomous terminal, distributed operation, multihop routing, dynamic network topology, fluctuating link capacity and light weight terminals. Routing protocol, security, medium access scheme, energy management, quality of service, self organization, protocol multicasting, scalability are some of the challenges that are taken into account for designing a MANET. Dynamic behavior, link stability, node mobility and frequently changing topology of MANET make the routing core issue. An effective routing algorithm helps to extend the successful deployment of mobile ad hoc networks.

INTRUSION DETECTION SYSTEM IN MANET

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Detection System (IDS) should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at first time. In this section, we mainly describe three existing approaches, namely, Watchdog [6], TWOACK [7] and AACK [2].

Watchdog and Pathrater

Marti et al. [6] proposed a scheme named Watchdog that aims to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Pathrater. Watchdog serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a pre-defined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Nevertheless, as pointed out by Marti *et al.*, the 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.

TWOACK

With respect to the six weaknesses of Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al. [7] is one of the most important one among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a 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.

AACK

Based on TWOACK, a new scheme called Adaptive ACKnowledgement (AACK) was proposed was proposed by A. Al-Roubaiey et al. [2]. Similar to TWOACK, AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

EAACK

After AACK scheme, E.M. Shakshuki et al. [1] proposed Enhanced Adaptive ACKnowledgement (EAACK) scheme, they introduce digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consists of three parts, namely, ACK, secure-ACK (S-ACK) and misbehavior report authentication (MRA). ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. S-ACK is an improved version of the TWOACK scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious.

RELATED WORK

Evaluating and Comparison of Intrusion in MANET

Prevention methods like authentication and cryptography techniques alone are not able to provide the security. Intrusion detection can be classified in two classes [5] based on data collection mechanisms and based on detection techniques Based on detection techniques: there are three board categories: misuse detection, anomaly detection, and specification-based detection.

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Mitigating Routing Misbehavior in MANET

Two techniques are used to improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. Detect misbehaving nodes. One solution to misbehaving nodes is to forward packets only through nodes that share a priori trust relationship. Another solution to misbehaving nodes is to isolate these nodes from actual routing protocols for the network. The techniques used are to detect the presence of nodes that agree to forward packets but fail to do so. Here watchdog is used, that identifies misbehaving nodes and a Pathrater that helps routing protocols avoid these nodes. The two techniques increase throughput and the overhead transmission.

New Trust based Security Method for MANET

Secure routing is the milestone in mobile ad hoc networks. Routing is always the most significant part for any networks. A trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. Trust management is a multifunctional control mechanism. It uses trust values to favor packet forwarding by maintaining a trust counter for each node[10]. A trust based security protocol attains confidentiality and authentication of packets in both routing and link layers of MANETs. A node will be punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious.

An Intrusion Detection System for MANET

An enhancement of the Watchdog/ Pathrater form of Intrusion Detection in Mobile wireless Ad hoc networks

(MANET).They describe about attacks mainly

- Route logic compromise

  EG: Misrouting, Black Hole
- Traffic pattern distortion

  EG: Packet Dropping, Packet Generation
- Routing protocols in ad-hoc networks
- Routing protocols in ad-hoc networks with security

Detecting and Preventing Attack using NIDSs

A Network Intrusion Detection System is used to monitor networks for attacks or intrusions. The network is also a pathway for intrusion. It follows the signature based IDs methodology for ascertaining attacks. It is an alert device in the event of attacks directed towards an entire network. It successfully captures packets transmitted over the entire network by promiscuous mode of operation and compares the traffic with crafted attack signatures. It also incorporates functionality to detect installed adapters on the system, selecting adapter for capture, pause capture and clearing captured data is shown in the screen shots.

EXISTING SYSTEM

To introduce new approach to the preceding approaches of intrusion detection system EAACK was introduced using digital signatures and RSA concepts. EAACK is an acknowledgement based IDS. EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted.

PROPOSED SYSTEM

As the existing approach had defects, a new scheme can be proposed where all acknowledgement packets will be encrypted as well as also provide integrity using 3GPP algorithm. The algorithm named as confidentiality (f8) for encryption and integrity (f9) for authentication. These algorithms provide a high level of security within the 3GPP context, meet their implementation requirements- in particular, allow a low power, low gate count implementation in hardware. The designers have therefore deliberately avoided over-designing the algorithm. They wanted the algorithms to be secure against all practical attacks, and carefully decided not to over-complicate them just to provide a very high security margin against unrealistic theoretical attacks. Types of attack against the underlying block cipher KASUMI were particularly considered: linear cryptanalysis, differential cryptanalysis, and variants such as impossible differentials, “miss in the middle”, etc, higher order differential cryptanalysis and interpolation, including probabilistic higher order analysis, identifying any classes of weak keys. Proposed scheme is a hybrid cryptographic scheme that uses both f8 algorithm for secure communication and f9 algorithm to authenticate other nodes.

CONCLUSION

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

In this paper, we have discussed some of the IDSs in MANET with their merits and demerits. As we know Packet dropping attack has always been a major threat to the security in MANETs. We are proposing a scheme using the f8 and f9 algorithms to provide the confidentiality and authenticity, respectively, in concern to security in MANET.

REFERENCES

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE, "EAACK – A Secure Intrusion Detection System for MANETs", in IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, 26th April 2012, VOL. 60, NO. 3, MARCH 2013.

[2] A. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki and H. Mouftah, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", in 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[3] U. Sharmila Begam1 and Dr. G. Murugaboopathi, "A RECENT SECURE INTRUSION DETECTION SYSTEM FOR MANETS", in IJETAE, Volume 3, Special Issue 1, January 2013

[4] Khairul Azmi Abu Bakar and James Irvine, "A Scheme for Detecting Selfish Nodes in MANETs using OMNET++", in Sixth International Conference on Wireless and Mobile Communications, 2010.

[5] Ms Shyama Sudarsan, Mrs Vinodhini and Dr S.Karthik, "Enhancing Key Management In Intrusion Detection System For Manets", in IJARCET, Volume 1, Issue 8, October 2012.

[6] S. Marti, T. J. Giuli, K. lai and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", in ACM, 2000.

[7] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs", in IEEE Transaction on Mobile Computing, VOL. 6, NO. 5, May 2007.

Author' biography with Photo

Monika Garg, pursuing Master's Degree Program from Lovely Professional University, Phagwara, Punjab, India. She received the B.Tech degree from Ideal Institute of Technology, Ghaziabad, affiliated to GBTU, U.P., India, in 2010. Her research interests include Mobile Ad-Hoc Network and Data structures.

Ms. Karanvir Kaur is presently an Assistant Professor in Lovely Professional University, Phagwara, Punjab, India. She received the M.E degree from Punjab University, Chandigarh. Her research interests include Mobile Ad-Hoc Network, Data mining, Data Structures, and Cloud Computing. She published paper in National and International conferences.

Simerpreet Kaur , pusuing Master's Degree from Lovely Professional University, Phagwara, Punjab, India.She received the B.Tech degree from H.P.U, Shimla, H.P, India.Her research interess include Sensor Networks and Neural Network.