International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 10 Issue 1 –OCTOBER 2014.

Malicious Detection for Security in Mobile Ad-hoc Network using EAACK

R.Biruntha[#1], K.K.Kavitha[*2] and C.Anitha[*3]

[#]*PG Scholar (M.Phil-CS), Selvamm Arts and Science College (Autonomous, Namakkal, Tamilnadu, India*
[*2]*Head of the Department (CS), Selvamm Arts and Science College (Autonomous), Namakkal, Tamilnadu, India*
[*3]*Assistant Professor (CS), Selvamm Arts and Science College (Autonomous, Namakkal, Tamilnadu, India*

Abstract— Discuss security issues and their current solutions in the mobile ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network Packet-dropping attack has always been a major threat to the security in MANETs. It has proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. In an effort to prevent the attackers from initiating forged acknowledgment attacks, it extended to incorporate digital signature in our proposed scheme.

Key Words: Mobile Ad Hoc Network, Security, Intrusion Detection, Secure Routing

I. INTRODUCTION

A mobile ad-hoc network is a infrastructure less networks of mobile devices connected by wireless. Each device in a MANET is free to move in any direction, and change its links to other devices frequently. Each node in the network acts as a router, forwarding data packets for other nodes. Vehicular Ad hoc Networks (VANETs) VANET are used for communication among vehicles and between vehicles and roadside equipment. Internet Based Mobile Ad hoc Networks (iMANETs) MANET links the mobile nodes and fixed Internet-gateway Nodes. Intelligent Vehicular ad hoc networks (InVANETs) This kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc. Intrusion detection is not a new concept in the network research. According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [4]. Although there are some differences between the traditional wired network and the mobile ad hoc network intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. In the following, we discuss some typical intrusion detection techniques in the mobile ad hoc networks in details.

FEATURES

Unreliability of wireless links between nodes because of the limited energy supply for the wireless nodes and the mobility of the nodes. Due to the continuous motion of nodes, the nodes can continuously move into and out of radio range of the other nodes in the ad hoc network and the routing information will be changing all the time because of the movement of the nodes. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issues so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Due to less infrastructure and easy deployment their applicability is scalable to be used.

II. 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 no cooperative 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.

2.1 DISADVANTAGES OF EXISTING SYSTEM:

Watchdog scheme fails to detect malicious misbehaviours 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.

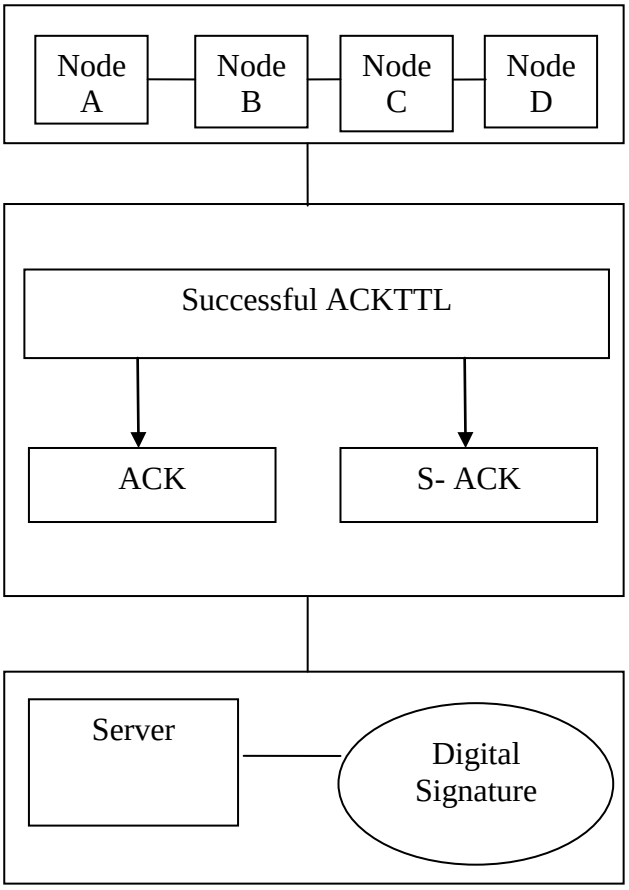
The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

III. PROPOSED SYSTEM

In this part, we mainly discuss various secure routing techniques that can help ensure the ad hoc routing security. Some of them deal with specific attacks that aim to disturb the ad hoc routing services, and provide some solutions to help defend against these attacks; whereas other techniques try to provide some effective tools or schemes to protect the ad hoc routing services from all kinds of attacks. Because routing service is one of the most important network services in the mobile ad hoc networks, there may be newly emerging attack types against the ad hoc routing all the time. Thus we need to constantly find new solutions to defend the ad hoc routing service against them. We mainly discuss two kinds of popular security techniques in the mobile ad hoc network, which are intrusion detection techniques and secure routing techniques. In each of the security schemes, several specific methods are pointed out and compared with each other. There are some points that some of the methods lack of, which are based on our observations. Therefore, we point out some aspects that may be further explored for some of the methods we have mentioned in this subsection. We survey the security solutions in the mobile ad hoc networks. First we analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security issues in the mobile ad hoc networks. We then point out various attack types that mainly threaten the mobile ad hoc networks. According to these attack types, we survey several security schemes that can partly solve the security problems in the mobile ad hoc networks. 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).

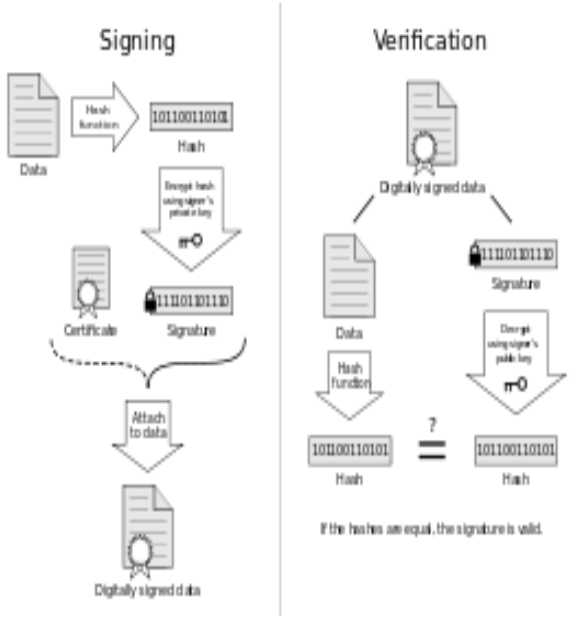
ADVANTAGES OF PROPOSED SYSTEM:

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.



ALGORITHM

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.



3.1 SIGNING

Let H be the hashing function and m the message:

Generate a random per-message value k where $0 < k < q$

Calculate $r = \left(g^k \bmod p\right) \bmod q$

In the unlikely case that $r = 0$, start again with a different random k

Calculate $s = k^{-1}\left(H\left(m\right) + xr\right) \bmod q$

In the unlikely case that $s = 0$, start again with a different random k

The signature is (r, s)

The first two steps amount to creating a new per-message key. The modular exponentiation here is the most computationally expensive part of the signing operation, and it may be computed before the message hash is known. The modular inverse $k^{-1} \bmod q$ is the second most expensive part, and it may also be computed before the message hash is known.

3.2 VERIFYING

Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.

Calculate $w = s^{-1} \bmod q$

Calculate $u_1 = H\left(m\right) \cdot w \bmod q$

Calculate $u_2 = r \cdot w \bmod q$

Calculate $v = \left(\left(g^{u1} y^{u2}\right) \bmod p\right) \bmod q$

The signature is valid if $v = r$

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

First, if g = h(p − 1)/q mod p it follows that gq ≡ hp − 1 ≡ 1 (mod p) by Fermat's little theorem. Since g > 1 and q is prime, g must have order q.

The signer computes

$$s = k^{-1}(H(m) + xr) \bmod q$$

Thus

$$\begin{aligned} k &\equiv H(m)s^{-1} + xrs^{-1} \\ &\equiv H(m)w + xrw \pmod q \end{aligned}$$

Since g has order q (mod p) we have

$$\begin{aligned} g^k &\equiv g^{H(m)w} g^{xrw} \\ &\equiv g^{H(m)w} y^{rw} \\ &\equiv g^{u1} y^{u2} \pmod p \end{aligned}$$

Finally, the correctness of DSA follows from

$$\begin{aligned} r &= (g^k \bmod p) \bmod q \\ &= (g^{u1} y^{u2} \bmod p) \bmod q \\ &= v \end{aligned}$$

IV. NETWORK CONSTRUCTION

In the network, numerous nodes are interconnected and exchange data or services directly with each other and construct a network topology to register the nodes. All systems have Connection with other systems. System details are maintained in the server system. It provides connection to the node whenever there is a request from another node. It's possible for a client to get more than one connection to the server. Create packet with IP header, data, and packet length. It receives the packets from source and analyses the packet header.

4.1UPLOAD & SEND FILES TO USERS

Every node on the path from the source node to the destination node becomes a cluster head, with the task of recruiting other nodes in its neighborhood and coordinating their transmissions. Consequently, the classical route from a source node to a sink node is replaced with a multi hop cooperative path, and the classical point-to-point communication is replaced with many-to-many cooperative communication.

4.2 MODIFICATION OF MESSAGES

This simply means that some parts of message are altered or the messages are changed or reordered.

4.3 DENIAL OF SERVICE

Is an attack that causes a loss of service to users, like loss of network connectivity and services, or overloading the computational resources? [3]

4.4 ATTACKS FROM MALICIOUS NODES

There are numerous kinds of attacks in the ad hoc network, almost all of which can be classified as the following two types:

I. External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

II. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node.

4.5 PASSIVE ATTACKS

This is an attack in which an unauthorized party gains access to an asset and does not modify its content. It try so extract the valuable information like node hierarchy.

Eavesdropping: The attacker monitors transmissions for message content.

Traffic Analysis: The attacker gains intelligence by monitoring the transmission and gaining information about the amount and sources of traffic.

V. INSTRUCTION DETECTION SYSTEM

Intrusion Detection System (IDS), generally detects unwanted manipulations to systems. IDS can be classified into three main categories as follows:

1. Signature or misuse based IDS uses pre-known attack scenarios and compare them with incoming packets traffic. There are several approaches in the signature detection, which differ in representation and matching algorithm employed to detect the intrusion patterns.
2. Anomaly based IDS attempts to detect activities that differ from the normal expected system behavior. This detection has several techniques, i.e.: statistics, neural networks, and other techniques such as immunology, data mining, and Chi-square test utilization.
3. Specification based IDS are hybrid of both the signature and the anomaly based IDS. It monitors the current behavior of systems according to specifications that describe desired functionality for security-critical entities. A mismatch between current behavior and the specifications will be reported as an attack.

VI. CONCLUSION AND FUTURE WORK

First we briefly introduce the basic characteristics of the mobile ad hoc network. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention. We then discuss some typical and dangerous vulnerabilities in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. The existence of these vulnerabilities has made it necessary to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks. Finally we introduce the current security solutions for the mobile ad hoc networks. We start with the discussion on the security criteria in mobile ad hoc network, which acts as a guidance to the security-related research works in this area. Then we talk about the main attack types that threaten the current mobile ad hoc networks. In the end, we discuss several security techniques that can help protect the mobile ad hoc networks from external and internal security threats. During the survey, we also find some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved. We will try to explore deeper in this research area

VII. REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Elec- tron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

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

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT ,Rohtak, Haryana,India, 2012, pp. 535–541.

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

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

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Model- ing and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind.Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand rout- ing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks rout-ing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582,2007.

AUTHOR'S DETAILS:

Mrs.K.K.Kavitha, MCA, M.Phil, Head of the Department, Department of Computer Science Selvamm Arts and Science College (Autonomous), kavithakkcs@gmail.com

Mrs.C.Anitha,MCA.,M.Phil., Assistant Professor, Department of Computer Science, Selvamm Arts and Science College (Autonomous), anithapnkl@gmail.com

R.Biruntha, Student, Department of Computer Science, Selvamm Arts and Science College (Autonomous) biruntha9842@gmail.com