ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Achieving a mechanism for detecting malicious nodes using Secure Acknowledgment (S-ACK)

ManojAithal S [1] ,Hemanth Kumar N.P [2]

M.Tech Scholar, Department of Computer Science and Engineering, Alva's Institute of Engineering and Technology Mijar, Mangalore, Karnataka, India[1]

Assistant Professor, Department of Computer Science and Engineering, Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India[2]

Abstract: Wireless communication represents a major industrial stake in the coming years. The mobility and scalability brought by wireless network made it possible in many applications. It targets applications in harsh environments such as war zones, emergency recovery, power plants and warships etc. MANETs is one among the wireless technology which is widely used. MANETs does not need any pre-configurations or permanent network architecture or infrastructure compared to wired technology. The wireless links between the nodes together with the dynamic-network nature of ad hoc network, increases the challenges of design and implement intrusion detection during the attacks. The intrusion detection system is achieved through a mechanism calledSecure Acknowledgment(S-ACK) which is more elegant than watchdog.

Index Terms: Mobile Ad hoc NETWORK (MANET), Watchdog, Secure Acknowledgment(S-ACK),Digital Signature.

I. INTRODUCTION

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. 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.

MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range.

In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation of MANETs.

II. SURVEY ON MANETs

A. Which wireless technology for industrial wireless sensor networks?

Wireless mesh networking has emerged in the recent years as a promising design paradigm for next-generation wireless communication networks with interesting characteristics such as self-organizing and auto-configurable topology, and *ad hoc* routing concept. These properties promise substantial benefits in terms of operating and maintenance costs of the communication infrastructure in industrial installations. They also ease the development of "killer applications" such as condition monitoring or condition-based maintenance (CBM) that requires flexible and cost-effective sensor networks. Wireless technologies help engineers achieve these objectives. However, most of the existing general-public wireless-communication technologies do not take into account the industrial requirements. There exists

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

proprietary radio-communication technologies for industrial use (e.g., Wavenis), but the benefits of interoperability (and thus, cost) are lost from multivendor solutions. Developing and promoting industrial wireless-communication standards help industrial end users preserve the expected benefits of wireless technologies. We propose to review the state of the art of current industrial wireless networking standards.

B. Denial of service attacks in wireless ad hoc networks

Due to the absence of a central trusted router in WANETs, nodes have to trust each other when routing data packets. The required mutual trust makes WANETs vulnerable to misbehaviors that may arise for several reasons:

1) Faulty nodes may misbehave due to configuration errors or some hardware errors.
2) Selfish nodes may not cooperate in network protocols in order to save energy.
3) Malicious nodes mount attacks with the intent of damaging the network or extracting valuable information from the network. Regardless of misbehavior type, it may cause a performance degradation of the whole network. Therefore, there is a need to secure network protocols in WANETs.

C. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks

Secure ad hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth an d the CPU processing capacity, memory, and battery power (energy) of each individual node in the network. Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information quickly as conditions change, requiring more rapid and often more frequent routing protocol interaction between nodes than is typical in a traditional (e.g ., wired an d stationary) network.

Expensive and cumbersome security mechanisms can delay or prevent such exchanges of routing information, leading to reduced routing effectiveness, and may consume excessive network or node resources, leading to many new opportunities for possible Denial-of-Service attacks through the routing protocol.

D. A survey on intrusion detection in mobile adhoc networks

Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system. Some assumptions are made in order for intrusion detection systems to work. The first assumption is that user and program activities are observable. The second assumption, which is more important, is that normal and intrusive activities must have distinct behaviors, as intrusion detection must capture and analyze system activity to determine if the system is under attack.

E. ad hoc mobile wireless networks routing protocols – a review

In general, on-demand reactive protocols are more efficient than proactive ones. On-demand protocols minimize control overhead and power consumption since routes are only established when required. By contrast, proactive protocols require periodic route updates to keep information current and consistent; in addition, maintain multiple routes that might never be needed, adding unnecessary routing overheads.

Proactive routing protocols provide better quality of service than on-demand protocols. As routing information is constantly updated in the proactive protocols, routes to every destination are always available and up-to-date, and hence end- to- end delay can be minimized. For on-demand protocols, the source node has to wait for the route to be discovered before communication can happen. This latency in route discovery might be intolerable for real-time communications.

In addition to proactive and reactive protocols, another class of unicast routing protocols that can be identified is that of hybrid protocols. The Zone- Based Hierarchical Link State Routing Protocol (ZRP) is an example of hybrid protocol that combines both proactive and reactive approaches thus trying to bring together the advantages of the two approaches.

ZRP defines around each node a zone that contains the neighbors within a given number of hops from the node. Proactive and reactive algorithms are used by the node to route packets within and outside the zone, respectively.

F. ARIADNE: a secure on-dem and routing protocol for a d hoc networks

Attacks on ad hoc network routing protocols generally fall into one of two categories: *routing disruption* attacks and *resource consumption* attacks. In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways.

In a resource consumption attack, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory (storage) or computation power.

From an application-layer perspective, both attacks are instances of a Denial-of-Service (DoS) attack.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

III. BACKGROUND STUDY

Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Path rater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission.

If a 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 predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field.

A. Disadvantages of Watchdog:

1) Ambiguous collisions.
2) Receiver collisions.
3) Limited transmission power.
4) False misbehavior report.
5) Collusion.
6) Partial dropping.

IV. PROPOSED SYSTEM

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation. Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation of MANETs.

A. Problem Statement

Watchdog which was the prominent IDS for MANETs until the minor flaws such as Ambiguous collisions, Receiver collisions etc. were detected. To overcome these flaws new mechanism is proposed

B. Objective

To develop an intrusion-detection mechanisms to protect MANET from attacks.

C. *Methodology*

S-ACK 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 packet transmitted over consecutive nodes along the path from the source to the destination.

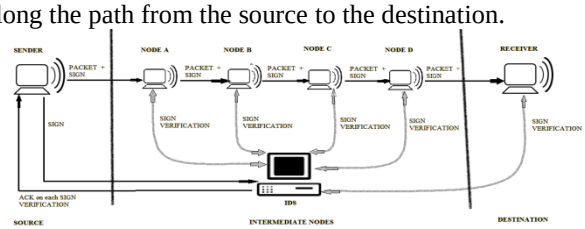

Fig 4.1 S-ACK scheme Architecture

V. SYSTEM DESIGN

UML has been developed as a languagefor modeling object- orientedsystems.Itsusehashoweverwidelybeen spread out.Today UML is usedfor system specifications. In different domains UML isused for specification and standardization of different systems or parts of the systems. UML is becoming a standard toolfor softwareandsystemengineers.

A. Dataflow diagram

A Data Flow Diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system, which can later be elaborated.

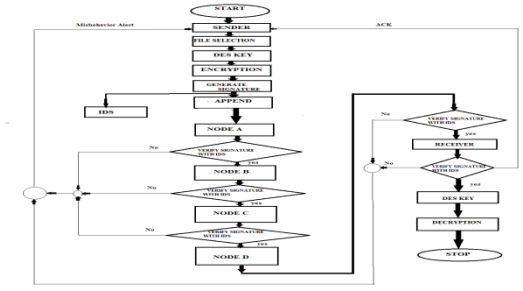

Fig 5.1 Dataflow diagram

The sender would select the file and would encrypt it using DES key. Then a signature is generated, which is sent to IDS (intrusion detection system) which plays a major role in transmitting of packets from source to destination. The encrypted file along with signature is transmitted to neighboring node (in this case let us consider Node A).In each intermediate nodes, signature verification is done with respect to IDS (intrusion detection system).

If the verification yields success then it is transmitted to next neighboring node else it would alert the sender of an intrusion or the misbehavior of the nodes.

VI. CONCLUSION AND FUTURE WORK

The project mainly deals with the IDS for MANETs and in proposed system it overcomes the most of the weakness of watchdog.

In future following works can be conducted:

1) Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

2) Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys.

REFERENCE

[1]. Which Wireless Technology forIndustrial Wireless Sensor Networks? The Development of OCARI Technology Khaldoun Al Agha, Senior Member, IEEE, Marc-Henry Bertin, Tuan Dang, Member, IEEE,AlexandreGuitton, Member, IEEE, Pascale Minet, Thierry Val, and Jean-Baptiste Viollet.

[2]. EAACK—A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE.

[3]. A Survey on Intrusion Detection in Mobile Ad Hoc Networks Using Enhanced Adaptive Acknowledgment.

[4]. Wireless/Mobile Network Security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 170 – 196 °c 2006 Springer Chapter 7 A Survey on Intrusion Detection in Mobile Ad Hoc Networks

[5]. Distributed and Cooperative Hierarchical Intrusion Detection on MANETs

[6]. A Comparative Study of Secure Intrusion-Detection Systems for Discovering Malicious Nodes on MANETs

[7]. A Study On Enhanced Adaptive Acknowledge (EAACK) Scheme In Receiver Collisions – An IDS In Wireless Mobile Ad-Hoc Networks