ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 2, Ver. 2 (April - June 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Improved Intrusion Detection System (IDS) For Manets Using Digital Signature

[I]M.SATHISH KUMAR, [II]T.PARAMESWARAN
[I]PG Student, Dept. of CSE, Anna University Regional Centre, Coimbatore
[II]Assistant Professor, Dept. of CSE, Anna University Regional Centre, Coimbatore

Abstract
A Mobile Ad-hoc network (MANET) is an infrastructure-less network consisting of self-configuring mobile nodes associated by wireless links. Every single node works both as a transmitter and a receiver. Nodes communicate directly with each other when both within the same communication range. Otherwise, they use their neighbours to relay messages. MANETs are highly vulnerable for passive and active attacks because of their rapidly open medium, changing topology and no centralized monitoring. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. Advanced improvements in technology and cut in hardware costs look the current tendency of expanding in use of MANETs into industrial applications. We propose and implement an intrusion-detection system named Improved Intrusion Detection System (IIDS) for MANETs. Compared to existing approaches, IIDS shows higher malicious-behaviour-detection rates under certain circumstances while not greatly affecting the network performances.

Keywords
Digital Signature, Improved Intrusion Detection System, Manet, Security, EAACK.

I. Introduction

In the recent years, wireless technology has enjoyed a tremendous rise in popularity and usage, in the domain of networking. In MANETs, the participating nodes do not rely on any existing network infrastructure. A mobile ad hoc network consisted of wireless nodes that can be rapidly deployed as a multi-hop packet radio network without the aid of any existing network infrastructure or centralized administration. Therefore, the interconnections between nodes are capable of changing on continual and arbitrary basis. Nodes within with in a radio range communicate directly, otherwise use intermediate parties to relay data transmissions. Ad hoc networks have a wide array of military and commercial applications. In these applications installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure network was destroyed. However, this flexibility introduces new security risks. Since prevention techniques are not enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions. Intrusion detection for MANETs is a complex and difficult task mainly due to the nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. so, new approaches need to be developed or else existing approaches need to be adapted for MANETs. In this paper suggest one of the intrusion detection for MANETs using EAACK.

II. Intrusion Detection System

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. The development of IDS is motivated by the following factors:

- Existing systems have security was that render them susceptible to intrusions, and finding and fixing all these deficiencies are not feasible.
- It is almost impossible to have an fully secure system.
- Even some secure systems are vulnerable to insider attacks.
- Requires new techniques to defend against them.

An intrusion detection system is used to detect many types of malicious behaviours of nodes that can compromise the security and trust of a computer system. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET knows how to detect the attackers as soon as they enter the network, we will be able to completely remove the potential damages caused by compromised nodes at the first time. IDSs are a great complement to existing proactive approaches and they usually act as the second layer in MANETs. There is a need for IDS to implement an intelligent control mechanism in order to monitor and recognize security breach attempts efficiently over a period of the expected network lifetime. The present research mechanism has focused on designing Intrusion Detection Systems (IDS) to monitor and analyse system events for detecting network resource misuse in a MANET .It is expected that the main text will be divided into several sections and subsections as author wishes. Make sure your breakdown of the main body does not affect the coherence of the flow of arguments or the continuity of the presentation. It may be a good idea to use appendixes for describing lengthy expressions / proofs/ or anything that might influence the readability of the main text.

A. Issues in Intrusion Detection System

Even though there are many proposed IDSs for wired networks, MANET's specific features make conventional IDSs ineffective and inefficient for this new environment. Researchers have been working recently on developing new IDSs for MANETs or changing the current IDSs to be suitable to MANETs. There are some new issues which should be taken into account when a new ID is being designed for MANETs.

- Lack of central points: MANETs do not have any entry points such as routers, gateways, etc. present in wired network. These can be used to monitor all network traffic that passes through them. A node in a MANET can see only a portion of a network: the packets it sends or receives together with other packets within its radio range.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

- Mobility: MANET nodes can leave and join the network and move independently at any time, so the network topology can change frequently. MANET can cause traditional techniques of IDS to be unreliable by its highly dynamic operation.

- Limited Resources: Mobile nodes generally use battery power and having different capacities. MANET devices are generally varied, e.g. laptops, hand held devices like PDAs, and mobile phones etc. The computational and storage capacities also varied. The variety of nodes, with scarce resources, affects effectiveness and efficiency of the IDS agents they support.

III. Existing System

As discussed before, due to the limitations of most MANET, nodes of MANETs assume that other nodes always cooperate with each other to relay data. This assumption makes the attackers with the opportunities to achieve significant impact on the network with just one or more compromised nodes. To address this problem, IDS should be added to enhance the security level of MA-NETs. 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. IDSs usually act as the second layer in MANETs. In this particular section, we describe three existing approaches, namely, Watchdog, TWOACK and AACK.

A. Watchdog

Watchdog that aims to improve throughput of net-work with the presence of malicious nodes. Actually, the watchdog scheme is consisting of two parts, called Watchdog and Path rather. Watchdog works as an intrusion detection system in MANETs. It is to detect the malicious nodes which are misbehaving in the network. Watchdog detects malicious node by promiscuously listens to its next hop's transmission. If Watchdog node detects that its next node fails to for-ward the packet within a certain period of time, it in-creases its failure counter.

In Watchdog, whenever a node's failure counter exceeds a pre-defined threshold, the node reports it as misbehaving. In future transmission, the Path rather cooperates with the routing protocols to avoid the reported nodes. Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many IDSs for MANET are either based on or developed as an improvement to the Watchdog scheme.

B. TWOACK

TWOACK is neither an enhancement nor a Watch-dog based scheme. Aiming to improve the performance of Watchdog, TWOACK acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination to detect misbehaving links. 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. TWOACK is required routing protocols such as Dynamic Source Routing (DSR) to work on.

The working process of TWOACK is, node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1,it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains route from node A to node C ,which is called reverse route and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. If this TWOACK packet is not received in a predefined time period, both nodes B and C are re-ported malicious. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a un-wanted network overhead. Due to the limited battery power nature of MANETs, redundant transmission process can easily degrade the life span of the entire network.

C. AACK

It is based on TWOACK Acknowledgement (AACK),AACK is an acknowledgement- based network layer scheme which can be considered as a combination of a scheme call ACK (identical toTWOACK) and an end-to-end acknowledgement scheme called ACK. When compared to TWOACK, AACK reduce the network overhead while still capable of maintaining or even surpassing the same network throughput.

Source node S will switch to TACK scheme by sending out a TACK packet. The network overhead is greatly reduced by this hybrid scheme in AACK, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgement packets. Many of the existing IDSs in MANETs adopt acknowledgement based scheme, TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is necessary to guarantee the acknowledgement packets are valid authentic.

IV. Proposed System

In this section, we describe our proposed Enhanced Adaptive Acknowledgement (EAACK) scheme in de-tails. The backbone of EAACK was proposed and evaluated through implementation. In this work, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehaviour report attack. a new intrusion detection system specially designed for MANETs, which solves false misbehaviour problem.

Initially, in ACK scheme source node send data packet to the destination through a route discovered using DSR .If the source node receive the acknowledgement from the destination within a particular time, it continue its next transaction.otherwise,source node switch into S-ACK scheme.

In S-ACK mode, every three consecutive nodes work in a group to detect misbehaving nodes. Detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. When a node forwards a data packet to its next hop, it verifies the arrival of this packet by requiring acknowledgement from the node that is two hops away from itself down the route. When the source node receives such misbehaviour report, instead of instantly trusting the report, MRA scheme is initiated to verify the correctness of such malicious report.

The concept of MRA scheme is to authenticate whether the destination node has received the reported missing packet. Due to the nature of ad hoc network, it is common to have multiple routes from one node to another. By adopting an alternative route

to the destination node, we circumvent the false misbehaviour reporter. The MRA packet contains the ID of the packet that has been reported dropped. When the destination node receives the MRA packet, it is required to search its local knowledgebase and see if there is a match of the reported packet. If it already existed, then we can conclude that the reported dropped packets have been received and whoever sends out this misbehaviour report is malicious. Otherwise, the misbehaviour report is trusted. The destination node acknowledges the source node by sending back an MRA acknowledgement packet. The malicious nodes are can be easily detected by neighbour nodes. So it is trusted method of malicious node detection.

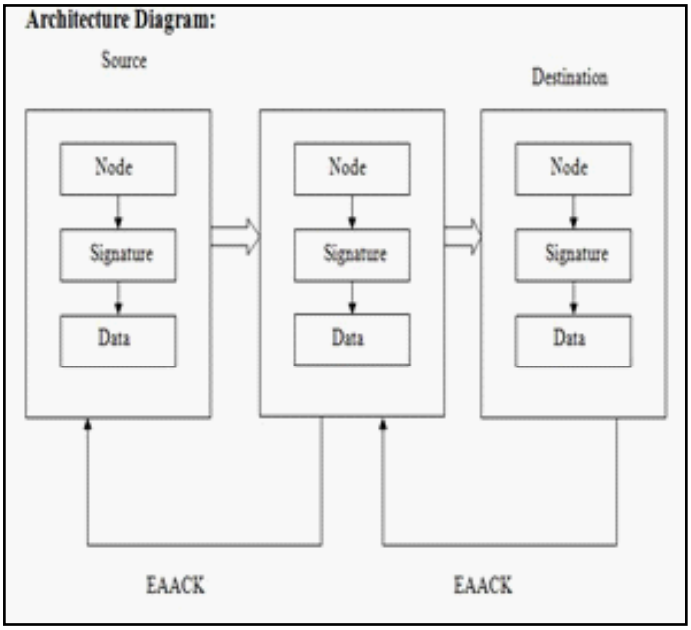

Fig.1: Enhanced Adaptive Acknowledgement

A. Network Topology

In our first module, we have to establish the Network. In this network, can have created the N nodes. These nodes are used to communicating each other indirectly to through the neighbour nodes. Using multicast socket, all nodes are used to detect the neighbour nodes.

B. ACK and S-ACK Scheme

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected. S-ACK scheme is an improved version of TWOACK scheme.
The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement 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.

C. MRA and Digital Signature Scheme

The Misbehaviour Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. False misbehaviour report can be generated by malicious attackers to falsely report that innocent nodes as malicious.
To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. The Digital Signature requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted. The goal is to find the most optimal solution for using digital signature in MANETs.

V. Conclusion and Future Work

Packet dropping attack has been one of the major threats to MANETs. In order to prevent and eliminate packet dropping attack, various approaches have been proposed. But, none of the existing approaches address the problem when the attackers are smart enough to forge acknowledgement packet or send out false acknowledgement. EAACK stands for Enhanced Adaptive Acknowledgement mechanism. It is an enhancement on Adaptive Acknowledgement scheme (AACK).We extended AACK to a new level where EAACK is capable of detecting forged acknowledgement packet or false misbehavior report.EAACK has the highest packet delivery ratio. Even though EAACK produces a considerable amount of network overhead in some scenarios, we believe our proposed scheme is valuable when security is of top concern.
This paper can be consider the following issues in the future research:

- Avoid the requirement of pre distributed keys by a doping a key exchange mechanism
- Testing the performance in real network environment instead of software simulation.

References

[1] *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.*
[2] *T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer- Verlag, 2008., pp. 4258–4265, Oct. 2009.*
[3] *M. Burmester and T. van Le, Secure multipath communication in mobile ad hoc networks, Proc. of ITCC'04 (Las Vegas), IEEE, April 2004.*
[4] *W. Du, L. Fang, and P. Ning, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," the 19th International Parallel and Distributed Priocessing Symposium (IPDPS'05), April 3 – 8, 2005, Denver, Colorado, USA.*
[5] *D. Johnson and D. Maltz. Dynamic Source Routing in Ad hoc Wireless Networks. Mobile Computing, Kluwer Academic Publishers, Chapter 5, pp. 153-181, 1996.*
[6] *M. Just, E. Kranakis, and T. Wan, "Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks," Proc. Int'l Conf. Ad-Hoc Networks and Wireless (ADHOCNOW '03), 2003.*
[7] *C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Journal of Ad Hoc Networks, Elsevier, 2003*
[8] *K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan. An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs. In the IEEE Transactions on Mobile Computing, vol. 6, pp. 536-550, 2007.*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[9] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehaviour in Mobile Ad hoc Networks. In the Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00, ACM), pp. 255-265, Boston, Massachusetts, US, 2000.

[10] Liu, K. Deng, J P. Varshney, K and Balakrishnan, K.2007 An acknowledgment-based approach for the detection of routing misbehavior in MANETs in IEEE Trans. Mobile Computer.