Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.209 – 215

RESEARCH ARTICLE

AN ACKNOWLEDGEMENT BASED APPROACH FOR DETECTING FALSE MISBEHAVIOUR IN MANETS

Mrs. I.Mettildha Mary, Ragavi.E, Renuga.K, Sasmitha.N, Veenalakshmi.R

Information Technology, Sri Ramakrishna Engineering College, Coimbatore, India

mettilda.lawrance@srec.ac.in, ragavi6194@gmail.com, renukrish18@gmail.com,

sasmithanagesh@gmail.com, veena.1105157@srec.ac.in

***Abstract*— Mobile Ad hoc NETwork (MANET) is one of the most important one among various wireless communication mechanisms. Its unique infrastructure less network and self-configuring capability makes it ideal for many mission critical applications. However, these characteristics also make MANET vulnerable to passive and active attacks due to its open medium, changing topology and lack of centralized monitoring. This leads to the need of a new intrusion detection system specially designed for mobile ad hoc networks. The proposed scheme introduces an approach to identify and detect misbehaving nodes in mobile ad hoc networks.**

***Keywords*— Digital signature, Digital Signature Algorithm (DSA), Enhanced Adaptive ACKnowledgement (EAACK), Mobile Ad hoc NETwork (MANET), Distance Source Routing (DSR)**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". 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. MANET has mobile nodes and router as shown in Fig 1

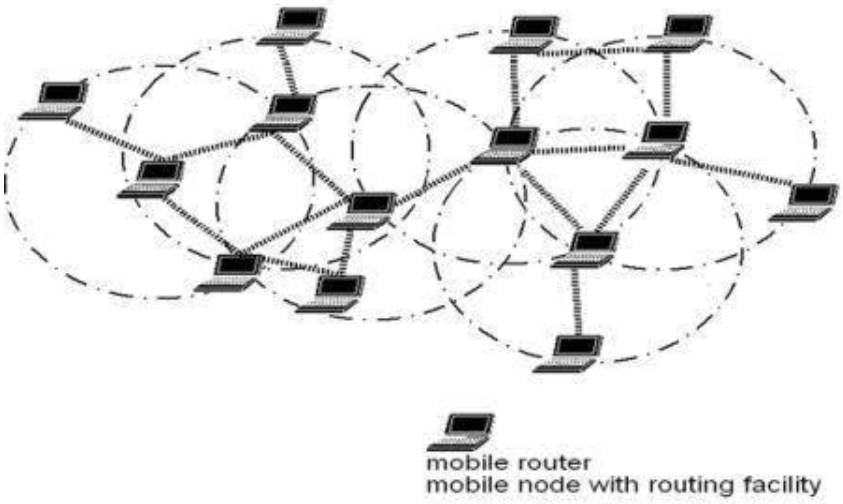

Fig. 1 Structure of MANET

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 (to determine, optimize, and distribute the routing table). MANETs are mobile and 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.

A. Advantages of MANET

MANETs are infrastructure less networks without any backbone and access points. They provide access to information and services regardless of geographic position. They have Independence from central network administration and are Self-configuring network in which nodes are also act as routers. Less expensive as compared to wired network. They possess improved flexibility and are robust due to decentralized administration. The network can be set up at any place and time.

B. Challenges in MANET

- **Limited bandwidth**

Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

- **Dynamic topology**

Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

- **Routing Overhead**

In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

- **Hidden terminal problem**

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

- **Packet losses due to transmission errors**

Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, unidirectional links, frequent path breaks due to mobility of nodes.

- **Mobility-induced route changes**

The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

- **Battery constraints**

Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

- **Security threats**

The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

II. VULNERABILITIES OF MOBILE AD HOC NETWORKS

Mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. The meaning of this vulnerability is self-evident: there is not such a clear secure *boundary* in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network.

In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses.

There are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, leakage of secret information, data tampering, message replay, message contamination, and denial of service. Due to MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such cases, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

III. NEED FOR AN EFFECTIVE INTRUSION DETECTION SYSTEM

Ad hoc networks like MANET does not require a fixed infrastructure and 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.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. 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 such cases, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

To address the problem of detecting the actual malicious nodes from the ones which have been falsely believed to be misbehaving with the help of EAACK scheme. EAACK is an acknowledgment-based IDS. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). All three parts of EAACK are acknowledgment based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. ACK acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected.

The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. In order to ensure that the acknowledgements packets are not forged, the packets are digitally signed using DSA algorithm.

IV. LIMITATIONS IN THE EXISTING SCHEMES

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, an 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 the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches.

A. Watchdog Scheme

Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an 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 [4]. 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 Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

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.

B. TWOACK

TWOACK detects misbehaving links by acknowledging every data packet transmitted over every 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 acknowledgment packet to the node that is two hops away from it down the route. 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. TWOACK solves two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack.

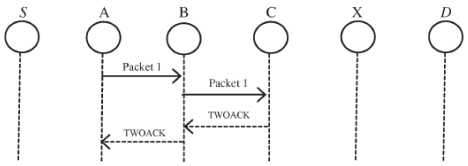

Fig.2 TWOACK Scheme

V. EFFECTIVE INTRUSION DETECTION SYSTEM FOR MANET

A new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem is EAACK(Enhanced Adaptive Acknowledgment) system [7]. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

A. EAACK

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. In case of misbehavior, it will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route. The S-ACK scheme 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 core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

B. PSR Technique

A lightweight proactive source routing (PSR) protocol is to facilitate opportunistic data forwarding in MANETs. In PSR, each node maintains a breadth-first search spanning tree of the network rooted at itself. This information is periodically exchanged among neighboring nodes for updated network topology information. Thus, PSR allows a node to have full-path information to all other nodes in the network, although the communication cost is only linear to the number of the nodes. This allows it to support both source routing and conventional IP forwarding.

PSR provides every node with a breadth-first spanning tree (BFST) of the entire networks are rooted at itself. To do that, nodes periodically broadcast the tree structure to their best knowledge in each iterations. Based on the information collected from neighbors during the most recent iteration, a node can expand and refresh its knowledge about the network topology by constructing a deeper and more recent BFST. This knowledge will be distributed to its neighbors in the next round of operation Route Update Due to its proactive nature, the update operation of PSR is iterative and distributed among all nodes in the network. At the beginning, node v is only aware of the existence of itself. Therefore, there is only a single node in its BFST, which is root node v. By exchanging the BFSTs with the neighbors, it is able to construct a BFST within N [v], i.e., the star graph centered at v, which is denoted Sv. In each subsequent iterations, nodes exchange their spanning trees with their neighbors. From the perspective of node v, toward the end of each operation interval, it has received a set of routing messages from its neighbors packaging the BFSTs. Note that, in fact, more nodes may be situated within the transmission range of v, but their periodic updates were not received by v due to, for example, bad

channel conditions. After all, the definition of a neighbor in MANETs is a fickle one. We have more details on how we handle lost neighbors subsequently. Node v incorporates the most recent information from each neighbor to update its own BFST. It then broadcasts this tree to its neighbors at the end of the period.

C. Neighborhood Trimming

The periodically broadcast routing messages in PSR also double as "hello" messages for a node to identify which other nodes are its neighbors. When a neighbor is deemed lost, its contribution to the network connectivity should be removed; this process is called neighbor trimming. Consider node v. The neighbor trimming procedure is triggered at v about neighbor u either by the following cases:

1) No routing update or data packet has been received from this neighbor for a given period of time.
2) A data transmission to node u has failed, as reported by the link layer.

D. Streamlined Differential Update

Route updates as hello messages in PSR, we interleave the "full dump" routing messages, as stated previously, with "differential updates." The basic idea is to send the full update messages less frequently than shorter messages containing the difference between the current and previous knowledge of a node's routing module. Both the benefit of this approach and balancing between these two types of messages have been extensively studied in earlier proactive routing protocols. The routing updates are in two new avenues. First, we use a compact tree representation in full-dump and differential update messages to halve the size of these messages. Second, every node attempts to maintain an updated BFST as the network changes so that the differential update messages are even shorter Compact tree representation. For the full-dump messages, our goal is to broadcast the BFST information stored at a node to its neighbors in a short packet. To do that,we first convert the general rooted tree into a binary tree of the same size, e.g., s nodes, using left-child sibling representation. Then, we serialize the binary tree using a bit sequence of 34 × s bits, assuming that IPv4 is used. Specifically, we scan the binary tree layer by layer. When processing a node, we first include its IP address in the sequence.

The difference between two BFSTs can be represented by the set of nodes that have changed parents, which are essentially a set of edges connecting to the new parents. We observe that these edges are often clustered in groups. That is, many of them form a sizeable tree sub graph of the network. Similar to the case of full dump, rather than using a set of loose edges, we use a tree to package the edges are connected to each other. As a result, a differential update message usually contains a few small trees, and its size is noticeably shorter.

The size of a differential update is determined by how many edges it includes. Since there can be a large number of BFSTs rooted at a given node of the same graph, we need to alter the BFST maintained by a node as little as possible when changes are detected. To do that, we modify the computation described earlier here, such that a small portion of the tree needs to change either when a neighbor is lost or when it reports a new tree.

PSR's route messaging is designed to be very concise. First, it uses only one type of message, i.e., the periodic route update, both to exchange routing information and as hello beacon messages rather than packaging a set of discrete tree edges in the routing messages, we package a converted binary tree to reduce the size of the payload by about a half. Third, we interleave full-dump messages with differential updates so that, in relatively stable networks, the differential updates are much shorter than the full-dump messages. To further reduce the size of the differential updates, when a node maintains its routing tree as the network changes, it tries to minimize alteration of the tree.

VI. PERFORMACE EVALUATION AND SIMULATION RESULTS

Here we consider three measures of performance – end-to-end delay, packet delivery ratio and control overhead. It has been observed that delay between sending packets have been reduced compared to the EAACK scheme as shown in Fig 3. As a result of which the packet delivery ratio increases correspondingly as shown in Fig 4. Control Overhead which indicates the number of control request and the control reply has also been observed to be comparatively low as shown in Fig 5.

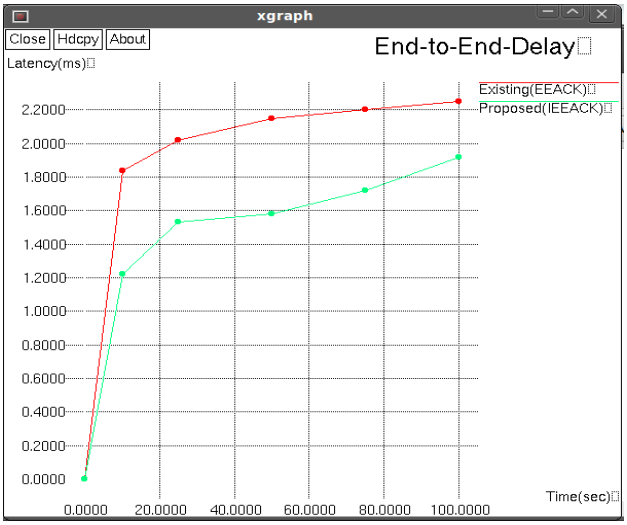

Fig.3. End-to-End Delay

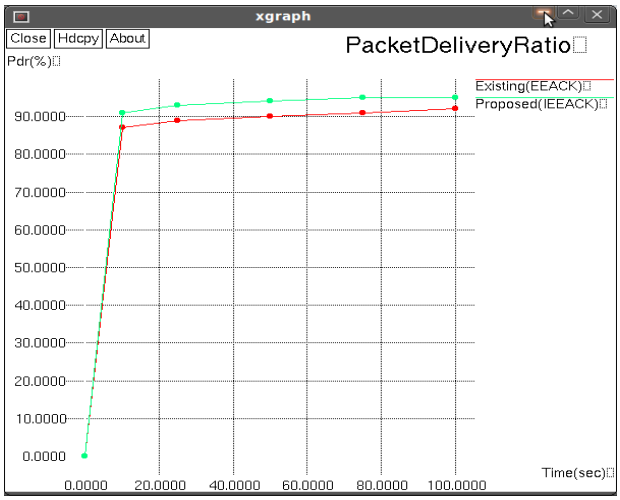

Fig.4. Packet Delivery Ratio

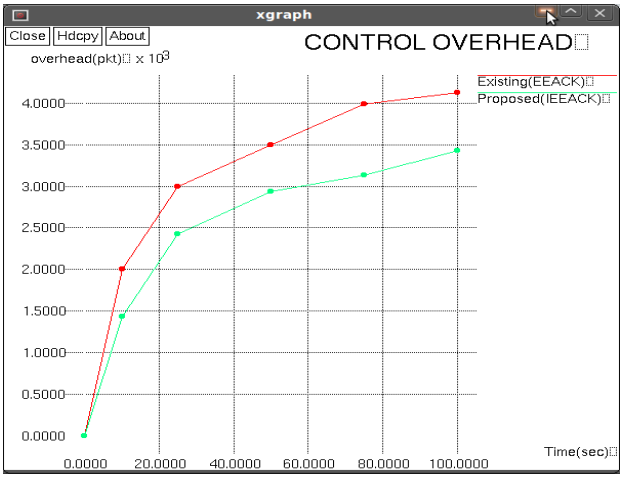

Fig.5. Control Overhead

VII. CONCLUSIONS

Compared with other approaches to combat the problem, such as the overhearing technique, the EAACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers. The EAACK scheme can be used as an add-on technique to routing protocols [1] [9] such as DSR [2] in MANETs. Extensive simulations of the EAACK scheme have been performed to evaluate its performance. Simulation results showed that the EAACK scheme maintains up to 91 percent packet delivery ratio even when there are 40 percent misbehaving nodes in the MANETs. The regular DSR scheme can only offer a packet delivery ratio of 40 percent. The false alarm rate and routing overhead of the EAACK scheme are investigated as well. One advantage of the EAACK scheme is its flexibility to control overhead with the use of the RACK parameter. In this work, only the link misbehavior is focused. It is more difficult to decide the behavior of a single node. This is mainly due to the fact that communication takes place between two nodes and is not the sole effort of a Single node. Therefore, care must be taken before punishing any node associated with the misbehaving links. When a link misbehaves, either of the two nodes associated with the link may be misbehaving. In order to decide the behavior of a node and punish it, it may be needed to check the behavior of links around that node. This is a potential direction for the future work.

REFERENCES

[1] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2003, pp. 12–23.

[2] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, ch. 5, 1998, pp. 153–181.

[3] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

[5] T. R. Andel and A. Yasinsac "Adaptive Threat Modeling for Secure Ad Hoc Routing Protocols", in Electronic Notes in Theoretical Computer Science, Volume 197, Issue 2, 2008 pp. 3-14.

[6] J. Cordasco and S. Wetze "Cryptographic Versus Trust-based Methods for MANET Routing Security" , in Electronic Notes in Theoretical Computer Science, Volume 197, Issue 2, 2008, pp. 131-140.

[7] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami "EAACK—A Secure Intrusion-Detection System for MANETs," in IEEE Transactions on Industrial Electronics, VOL. 60, NO. 3, 2013, pp.120-132.

[8] V. Daza, P. Morillo and C. Ràfols "On Dynamic Distribution of Private Keys over Manets" in Electronic Notes in Theoretical Computer Science, Volume 171, Issue 1,2007, pp. 33-41.

[9] Y. Hu, D. Johnson, and A. Perrig "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.* , 2000, pp. 3–13.

