An Intrusion Detection System for MANET against Selective Packet Dropping

Archana V
Master of Technology
Department of CSE
N.S.S College of Engineering
Palakkad-678001, Kerala, India

Maya Mohan
Assistant Professor,
Department of CSE
N.S.S College of Engineering
Palakkad-678001, Kerala, India

ABSTRACT
A MANET (mobile ad hoc network) is a self-configuring infrastructure-less network of mobile devices connected through a wireless medium. All the devices in MANET can move independently in any direction and frequently change its link to other devices. Each device can act as both a transmitter and receiver therefore MANET doesn't require a fixed network infrastructure. Self-configuring ability of MANET made it popular among critical mission applications like emergency recovery or military use. But MANET is vulnerable to malicious attackers due to open medium and wide distribution of the nodes. So, it's important to develop some efficient intrusion detection mechanisms to protect MANET from attacks. As a contribution to EAACK, an intrusion detection system for MANET a method is proposed to combat the selective packet dropping attack and reduce routing overhead and delay caused by EAACK. The proposed Intrusion Detection System for MANET against Selective Packet Dropping, as per the simulation results shows that it is efficient when compared to EAACK in case of select packet dropping attack and produces less RO and delay than EAACK.

General Terms
Security, MANET

Keywords
Enhanced Adaptive Acknowledgement (EAACK), Mobile Ad-hoc Network (MANET), Misbehavior Report Authentication (MRA), Routing Overhead (RO), Packet Delivery Ratio (PDR)

1. INTRODUCTION
A Mobile Adhoc Network is a collection of independent mobile nodes equipped with a wireless transmitter and receiver that can communicate via radio waves to each other directly or indirectly. MANET is of two types, single-hop and multi-hop. In a single-hop network nodes within the same radio range communicate directly with each other whereas in a multi-hop network nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. Figure 1 shows a simple ad-hoc network with 3 nodes. Nodes 1 and 3 are not within the range of each other however node 2 can be used to forward packets between node 1 and 3. The node 2 will act as a router and these three nodes together form mobile ad-hoc network.

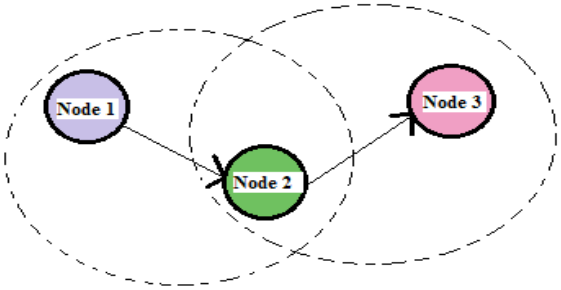

Fig 1: Example of mobile ad-hoc network

In MANET, nodes perform all networking functions such as routing and packet forwarding in a self-organizing manner. For these reasons, it's challenging to secure a mobile adhoc network. In the mobile ad hoc network, nodes join the network automatically. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The decentralized infrastructure makes MANET useful in critical mission applications like military conflict or emergency recovery. Due to minimal configuration and quick deployment nature

MANET can be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install like medical emergency situations, military conflicts, natural or human-induced disasters. Unfortunately, the remote distribution of mobile adhoc network and open medium make MANET vulnerable to attacks. For example, attackers can easily capture and compromise nodes to achieve attacks due to the nodes' lack of physical protection. In particular, most routing protocols in MANET assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, therefore attackers can easily compromise MANET by inserting non-cooperative or malicious nodes into the network. Therefore it is crucial to develop an intrusion-detection system specially designed for MANETs.

2. RELATED WORK
2.1 AACK
AACK is an acknowledgment-based network layer scheme which is combination of an end-to-end acknowledgment scheme called Acknowledge (ACK) and TACK. In the ACK scheme shown in Figure 1, the source node S sends the packet then all the intermediate nodes simply forwards this packet.

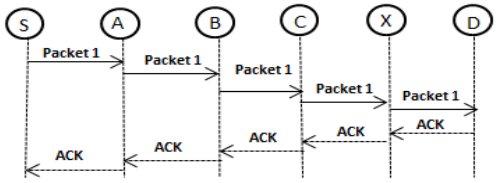

Fig 2: ACK scheme

On receiving packet destination is required to send back an acknowledgment packet to the source node S along the same route in reverse order. If the acknowledgment packet is received by the source node S within a predefined time period then the packet transmission from node S to node D is successful else the source node S will switch to TwoACK scheme and will send a TACK packet. Although adoption of a hybrid scheme greatly reduces the network overhead, AACK fail to detect malicious nodes in the presence of forged acknowledgment packets and false misbehavior report [9].

2.2 EAACK

EAACK (Enhanced Adaptive Acknowledgment) [1] tackles three weaknesses of Watchdog scheme, namely receiver collision, false misbehavior report and limited transmission power.

EAACK consists of three major parts, namely, ACK, Secure ACK (S-ACK), and Misbehavior Report Authentication (MRA). The results of EAACK demonstrated positive performances against other IDS in the cases of false misbehavior report, receiver collision and limited transmission power. EAACK incorporated digital signature in an effort to prevent the attackers from initiating attacks using forged acknowledgment. Although it generates more routing overhead in some cases, it can improve the network's PDR when the attackers are smart enough to forge acknowledgment packets.

3. SCHEME DESCRIPTION

This paper proposes a new routing mechanism to combat the common selective packet dropping attack. A selective packet dropping attack is a kind of denial of service where a malicious node attracts packets and drops them selectively without forwarding them to the destination. For example in Figure 3 node 1 is the source node, node 7 is the destination node and node 2 to 6 act as intermediate nodes. Node 5 is selective packet dropping node. When source node wishes to transmit data packet it will first send out RREQ packets to the neighboring nodes.

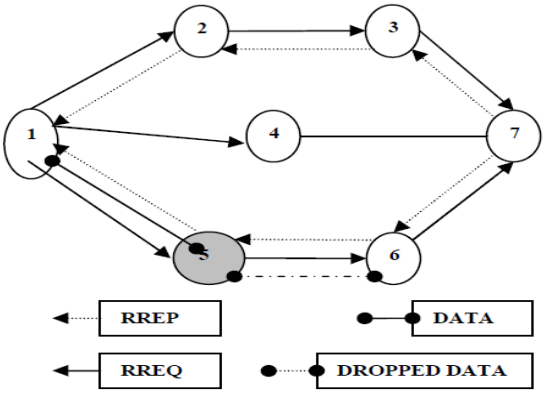

Fig 3: Selective packet dropping

The nodes which are malicious in the network also receive the RREQ packet. After receiving RREP from the destination source node will transmit data packets. As node 5 is also the part of routing path it will receive the data packets and drops some of them while forwarding others. This type of selective packet dropping attack is very hard to detect as the malicious nodes pretend to act like a good node. In this paper malicious nodes are identified and isolated by modifying the routing mechanism based on trust.

3.1 ACK implementation

ACK is an end to end acknowledgment scheme. ACK is part of hybrid scheme in EAACK aiming to reduce the network overhead when no network misbehavior is detected. In this mode, node S will send out an ACK data packet to destination Node D. Node D on receiving the packet will send an ACK acknowledgment packet to the source in reverse order along the same route. If node S receives ACK acknowledgment packet within predefined time period then the packet transmission from node S to node D is successful else node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

3.2 S-ACK

In S-ACK (Secure Acknowledgment) mode every three consecutive nodes work in a group to detect misbehaving nodes. The third node is required to send an acknowledgment packet to the first node for every three consecutive nodes in the route from source to destination. This mode can find misbehaving nodes in the presence of receiver collision and limited transmission power. By switching to MRA mode misbehavior report is confirmed.

3.3 MRA

The MRA (Misbehavior Report Authentication) scheme is designed to resolve the false misbehavior report attack where innocent nodes are reported as malicious by attackers .The core of MRA scheme is to authenticate whether the reported missing packet reached the destination node through a different route. In this mode, the source node will first search its local knowledge base and finds an alternative route to the destination node. It is common to find out multiple routes between two nodes due to the nature of MANETs. On receiving MRA packet the destination node will search its local knowledge base and finds whether the reported packet was already received or not . If already received then will conclude that this is a false misbehavior report and whoever generated this report will be marked as malicious else the misbehavior report will be trusted and accepted.

3.4 Digital Signature Validation

To detect misbehaviors in the network above three modes rely on acknowledgment packets. So it is important to ensure that all acknowledgment packets are untainted and authentic. If the attackers are smart enough to forge acknowledgment packets all of the three schemes will be vulnerable. Therefore to ensure the integrity it requires all acknowledgment packets to be digitally signed before they are sent out and verified. RSA digital signature scheme is used to ensure integrity.

3.5 Trust Identification

In this module, the trust between the nodes is calculated and based on that the nodes are classified into Unknown, Companion and Known.

UNKNOWN

- Node x never sent or received any messages to or from node y
- Trust levels between the nodes are very low.
- Probability of malicious behavior is high.
- Newly arrived nodes are grouped in to this category.

KNOWN

- Node x sent or received some messages to or from node y
- Trust levels between the nodes are neither low nor too high.
- Probability of malicious behavior is to be observed.

COMPANION

- Node x sent or received plenty of messages to or from node y
- Trust levels between the nodes are very high.
- Probability of malicious behavior is very low.

In this trust model, every node maintains a value (which we call trust value) for each of its neighbors (nodes that are within its radio range). This value is a measure of the level of trust it has on its neighbor. For scalability, trust model is designed such that the trust value is calculated using only local information. Let T_i (j) denote the level of trust of node i on neighbor j. T_i (j) is taken as the weighted average of two components.

$$T_i(j) = \alpha\, T_{i\,(self)}(j) + \beta\, T_{i\,(neighbor)}(j) \qquad (1)$$

$\alpha + \beta = 1$ and $0 \le \alpha, \beta \le 1$

$T_{i\,(self)}$ (j) represents the self-trust of node i on node j, based on node i's observation of node j's behavior (e.g. by monitoring traffic of node j).$T_{i\,(neighbor)}$ (j) represents the trust that neighbors of node i have on node j. These neighbors of node i are also neighbors of node j. Let a_1, a_2, a_3 . . . a_n be the neighbors of node i (where n is the number of neighbors) such that they are also neighbors of node j.

Then $T_{i\,(neighbor)}$ (j) is given by

$$T_{i\,(neighbor)}(j) = \frac{1}{n}\sum_{k=1}^{n} T_{a\,k\,(self)}(j) \qquad (2)$$

By varying the values of α and β, we can thus vary the weight of self-trust as compared to neighbors trust in evaluating the overall trust i.e., for nodes belonging to Unknown group neighboring trust is given weightage and for nodes belonging to Companion group self-trust is given weightage and for nodes of Known group equal weightage is given for self-trust and neighboring trust. It is clear that $T_{i\,(neighbor)}$ (j) is the average of the existing trusts of the neighbors. Thus, in node trust model, the past history is also taken into account. This is important when we want to evaluate trust based not only on present observations but also on past behavior. $T_{i\,(self)}$ (j) in (1) form the basic block upon which the model is built. The values of $T_{i\,(self)}$ (j) range from 0 (denoting absolutely no trust, Unknown) to 1 (denoting full trust, Companion).

For simplicity and also to minimize the overhead in a resource-constrained environment as that of a MANET, we have used only passive monitoring of forwarded data traffic to evaluate the behavior of a node. Subsequently, this behavior is translated to an estimate of the trust, which the monitoring node has on the monitored node. For each neighbor of a node, we define three data structures: (i) To forward, (ii) Forwarded and (iii) Source list. To forward and Forwarded data structures store the number of packets to be forwarded and the number of packets already forwarded, respectively. Based on monitoring whether nodes are forwarding all the packets or dropping some packets the self-trust $T_{i\,(self)}$ (j) is calculated. If a node is dropping some packets value of self-trust is based on the ratio of number of packets dropped to total number of packets to forward.

3.6 Trust Aware Routing

Based on the results of the trust calculation, trust aware routing module is made where the problem of packet dropping is avoided by making the transmission in the trust aware routing nodes. Proposed technique is incorporated in ad hoc on-demand vector routing (AODV) protocol. Whenever neighboring node is a companion data is transferred immediately which eliminates the overhead of invoking trust estimator between companions.

4. EVALUATION

NS2 (Network Simulator 2) is used to simulate the performance of EAACK under different types of attacks on a platform with GCC 4.3 and Ubuntu 11.04. In order to better compare simulation results with other research works, the default scenario settings in NS 2.28 are adopted

Simulation Parameters

- Simulation time : 10 mins
- Number of nodes : 50
- Topology area : 1611m x 766 m
- Mobility model : Random way point
- Traffic type : UDP
- Maximum speed : 20 m/s
- Packet size : 512 bytes for UDP
- Propagation : Two Ray Ground
- Channel type : Wireless channel

Maximum hops allowed in this configuration setting are four. Both physical layer and 802.11 MAC layer are included in the wireless extension of NS2.

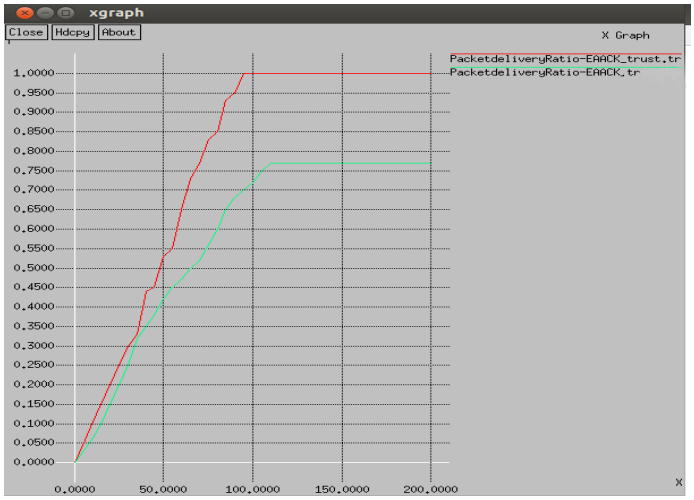

Fig 4: Simulation result for PDR

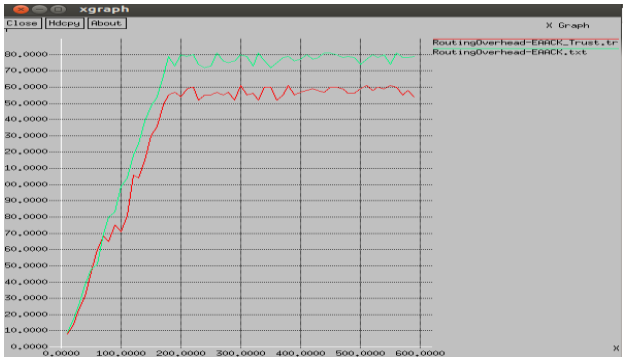

Fig 5: Simulation result for RO

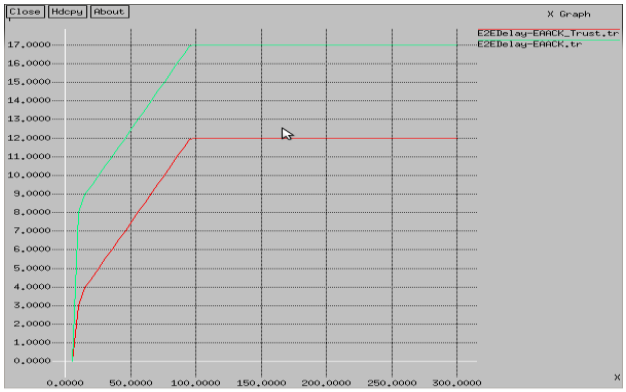

Fig 6: Simulation result for E2E Delay

Simulation results show that proposed system, An Intrusion Detection System for MANET against Selective Packet Dropping is efficient when compared to EAACK in case of select packet dropping attack. It produces less RO and delay than EAACK when there is known and companion nodes.

5. CONCLUSION

Due to dynamic topology, distributed operation and limited bandwidth MANET is more vulnerable to many attacks. As the use of mobile ad hoc networks (MANETs) has increased, security of MANETs has also become more important accordingly. Packet-dropping attack has always been a major threat to MANET's security. In this paper, robust trust-aware IDS specially designed for MANETs is proposed to over efficient packet dropping in MANET and reduce network overhead by considering association between nodes and compared it against other popular mechanisms in different scenarios through simulations. Simulation results show that proposed system is efficient compared to EAACK in case of selective packet dropping attack and it produces less RO and delay than EAACK when there is known and companion nodes.

6. REFERENCES

[1] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for MANETs." Industrial Electronics, IEEE Transactions on 60.3 (2013): 1089-1098.

[2] Anantvalee, Tiranuch, and Jie Wu. "A survey on intrusion detection in mobile ad hoc networks." Wireless Network Security. Springer US, 2007. 159-180.

[3] Kang, Nan, Elhadi M. Shakshuki, and Tarek R. Sheltami. "Detecting misbehaving nodes in MANETs." Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services. ACM, 2010.

[4] Kang, Nan, Elhadi M. Shakshuki, and Tarek R. Sheltami. "Detecting forged acknowledgements in MANETs." Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on. IEEE, 2011.

[5] Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." Mobile Computing, IEEE Transactions on 6.5 (2007): 536-550.

[6] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.

[7] Lee, Jin-Shyan. "A Petri net design of command filters for semiautonomous mobile sensor networks." Industrial Electronics, IEEE Transactions on 55.4 (2008): 1835-1841.

[8] Mishra, Amitabh, Ketan Nadkarni, and Animesh Patcha. "Intrusion detection in wireless ad hoc networks." Wireless Communications, IEEE 11.1 (2004): 48-60.

[9] Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol." Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. ACM, 2002.

[10] Michiardi, Pietro, and Refik Molva. "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks." Advanced Communications and Multimedia Security. Springer US, 2002. 107-121.

[11] Balakrishnan, Kashyap, Jing Deng, and Pramod K. Varshney. "TWOACK: preventing selfishness in mobile ad hoc networks." Wireless Communications and Networking Conference, 2005 IEEE. Vol. 4. IEEE, 2005.

[12] Hongwei, Ma. "The study on ad hoc networks security strategy based on Routing Protocols." Computer Science and Network Technology (ICCSNT), 2011 International Conference on. Vol. 1. IEEE, 2011.

[13] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[14] Frodigh, Magnus, Per Johansson, and Peter Larsson. "Wireless ad hoc networking-The art of networking without a network." Ericsson Review 4.4 (2000): 249.

[15] Yang, Hao, et al. "Security in mobile ad hoc networks: challenges and solutions." Wireless Communications, IEEE 11.1 (2004): 38-47.

[16] Chlamtac, Imrich, Marco Conti, and Jennifer J-N. Liu. "Mobile ad hoc networking: imperatives and challenges." Ad Hoc Networks 1.1 (2003): 13-64.

[17] Sun, Bo, Kui Wu, and Udo W. Pooch. "Alert aggregation in mobile ad hoc networks." Proceedings of the 2nd ACM workshop on Wireless security. ACM, 2003.

[18] Sterne, Daniel, et al. "A general cooperative intrusion detection architecture for MANETs." Information Assurance, 2005. Proceedings. Third IEEE International Workshop on. IEEE, 2005.

[19] Royer, Elizabeth M., and Chai-Keong Toh. "A review of current routing protocols for ad hoc mobile wireless

networks." Personal Communications, IEEE 6.2 (1999): 46-55.

[20] Aarti, Dr SS. "Tyagi,"Study Of Manet: Characteristics, Challenges, Application And Security Attacks"." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 252-257.

[21] Hinds, Alex, et al. "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)." International Journal of Information and Education Technology 3.1 (2013).

[22] Gagandeep, Aashima, and Pawan Kumar. "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review." International Journal of Engineering and Advanced Technology (IJEAT) 1.5 (2012).

[23] Wazid, Mohammad, Rajesh Kumar Singh, and R. H. Goudar. "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some available Detection Techniques." Proceedings published by International Journal of Computer Applications (IJCA) International Conference on Computer Communication and Networks CSI-COMNET, Hawaii. 2011.