International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.29 (2015)
© Research India Publications; http://www.ripublication.com/ijaer.htm

Energy aware Intrusion Detection System for MANETs

A.V.Santhosh Babu[1]
Assistant Professor / Dept. of Information Technology
Sengunthar College of Engineering[1]
Tamilnadu
santhosh.vadivalagan@gmail.com[1]

Dr.P.Meenakshi Devi[2]
Professor & Head / Department of Information Technology
K.S.R.Institute for Engineering and Technology
Tamilnadu
drpmeenakshidevi@gmail.com[2]

***Abstract*— An ad hoc network is the assortment of cooperative wireless nodes without existence of any central point or infrastructure. The network topologies dynamically change in an unpredictable manner. Because of these features it is now popular among critical mission applications like military use or emergency recovery. There also have 2 issues like Security and energy respectively. Since there is no central authority to manage the nodes in mantes, malicious attackers can easily capture and compromise nodes to achieve attacks. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. Also each node act both as transmitter and receiver, hence energy consumption is a major challenge in MANETS. Main focus of this paper is, with minimum energy detecting intrusion node by using the existing Enhanced Adaptive Acknowledgement (EAACK) scheme and the overhead is further reduced by using Zone based routing.**

Keywords*— *Zone Routing Protocol, Enhanced Adaptive Acknowledgement (EAACK), Intrusion Detection system (IDS), Mobile Ad hoc Network (MANET)

I. INTRODUCTION

Because of the independent nature, wireless networks have more attained more importance in the recent years. An ad hoc network is a set of wireless mobile nodes that forms a transitory network without any access point. Each node in the MANETs communicates through radio waves. Node within range can directly communicate, while the nodes outside the range establish communication through the intermediate nodes. Each node act as both transmitter and receiver. This idea of Mobile ad-hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. Fig 1. Shows a sample Manet environment.

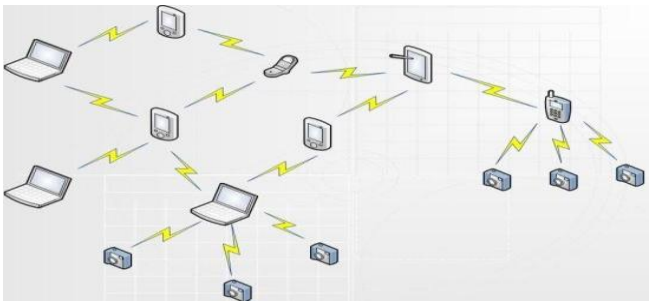

Fig. 1. Mobile Adhoc Network

Though MANETs have many advantages, recent research analysing the challenges in adopting Manets.

A. CHALLENGES IN MANETS

1) Limited radio range: Wireless link have lower coverage area than infrastructure networks. further fading, noise, and interference conditions, etc., occurs when the coverage area increases.

2) 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.

3) Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

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

5) 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.

In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of access point, routing overhead and energy constraint.

II. ANALYSIS OF EXISTING IDS IN MANET

As discussed above, due to the limitations of most MANET routing protocols, 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, 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 [1]. Anantvalee and Wu [2] presented a very thorough survey on contemporary IDSs in MANETs. In this section, it mainly describe the existing approaches, namely, Watchdog [3], TWOACK [4], Adaptive Acknowledgment (AACK) [5] and Enhanced Adaptive Acknowledgement (EAACK).[6]

1) For Watchdog: Marti et al. [3] Proposed a scheme named 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 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. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme [3], [7], [8], [9].

Nevertheless, as pointed out by Marti *et al.* [3], the 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.

2) TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al. [4] is one of the most important approaches among them. On the contrary to many other schemes, TWOACK 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 every three consecutive nodes along the path from the source to the destination.

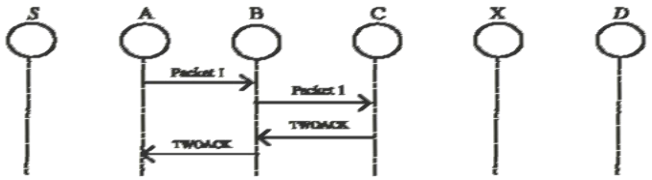

Fig. 2. The TWOACK Scheme

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. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process of TWOACK is shown in Fig. 2.

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, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of 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. However, many research studies are working in energy harvesting to deal with this problem [8], [9], [10].

3) AACK: Based on TWOACK, Sheltami et al. [5] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme which can be considered of a scheme called TACK (identical to TWOACK) and an end to end acknowledgement scheme called Acknowledgement (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintain or even surpassing the same network throughput.

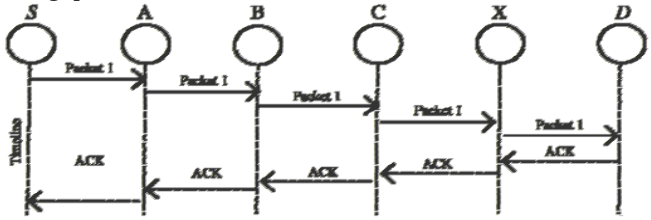

Fig. 3. The ACK Scheme

In the ACK scheme shown in Fig. 3, the source node S sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission

from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. 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. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

4) EAACK: To mainly address the problem of false misbehavior report and forged acknowledgement packets in TWOACK scheme, Elhadi, Nan Kang and Tarek proposed a scheme named Enhanced AACK (EAACK) [6]. It consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). ACK scheme acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.*

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 intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report. Since it is an acknowledgment based IDS, to ensure that all acknowledgment packets in EAACK are authentic and untainted, all acknowledgment packets are digitally signed before they are sent out and verified until they are accepted.EAACK is required to work on existing flat routing protocols such as Dynamic Source Routing[9]. Though it demonstrates positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report it generates more routing overhead in most of the cases.

By maintaining EAACK's ability to improve the network's Packet Delivery Ratio when the attackers are smart enough to forge Acknowledgement packets , we can considerably reduce the network energy consumption by subdividing the network into area(zone).Zone based routing reduces battery consumption drastically.

III. OVERVIEW OF ZRP

After the EAACK scheme surely is an effective IDS that can be used in MANETs. But, network overhead and limited transmission power are still a problem. It is mainly because all the nodes in the networks are equity, and functions as terminal as well router. There is difference in performance instead of function. The main advantage of the MANET structure is that there are multiple paths between source-destination pairs. So it can distribute traffic into multiple paths, decrease congestion and eliminate possible "bottleneck". But MANET with the plane structure will increase routing control overhead; the scalability problem is also likely to happen.

To put the related work in context, we first briefly describe the protocol we are working with, the Zone Routing Protocol and Optimized Link State Routing Protocol (OLSR)

The Zone Routing Protocol, as its name implies, is based on the concept of zones. A routing zone is defined for each node separately, and the zones of neighboring nodes overlap. The routing zone has a radius ρ expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most ρ hops. An example routing zone is shown in Fig. 4, where the routing zone of S includes the nodes A–I, but not K. In the illustrations, the radius is marked as a circle around the node in question. It should however be noted that the zone is defined in hops, not as a physical distance.

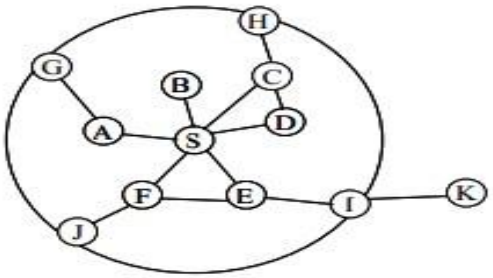

Fig. 4. Sample Zone routing protocol

The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius ρ. The nodes whose minimum distance is less than ρ are interior nodes. In Figure 1, the nodes A–F are interior nodes; the nodes G–J are peripheral nodes and the node K is outside the routing zone. Note that node H can be reached by two paths, one with length 2 and one with length 3 hops. The node is however within the zone, since the shortest path is less than or equal to the zone radius.

The number of nodes in the routing zone can be regulated by adjusting the transmission power of the nodes. Lowering the power reduces the number of nodes within direct reach and vice versa. The number of neighboring nodes should be sufficient to provide adequate reach ability and redundancy. On the other hand, a too large coverage results in many zone members and the update traffic becomes excessive. Further, large transmission coverage adds to the probability of local contention. ZRP refers to the locally proactive routing

component as the Intra-zone Routing Protocol (IARP). The globally reactive routing component is named Inter- zone Routing Protocol (IERP). IERP and IARP are not specific routing protocols. Instead, IARP is a family of limited-depth, proactive link-state routing protocols. IARP maintains routing information for nodes that are within the routing zone of the node. Correspondingly, IERP is a family of reactive routing protocols that offer enhanced route discovery and route maintenance services based on local connectivity monitored by IARP.

The fact that the topology of the local zone of each node is known can be used to reduce traffic when global route discovery is needed. Instead of broadcasting packets, ZRP uses a concept called border casting. Border casting utilizes the topology information provided by IARP to direct query request to the border of the zone. The border cast packet delivery service is provided by the Border cast Resolution Protocol (BRP). BRP uses a map of an extended routing zone to construct border cast trees for the query packets. Alternatively, it uses source routing based on the normal routing zone. By employing query control mechanisms, route requests can be directed away from areas of the network that already have been covered. In order to detect new neighbor nodes and link failures, the ZRP relies on a Neighbor Discovery Protocol (NDP) provided by the Media Access Control (MAC) layer. NDP transmits "HELLO" beacons at regular intervals. Upon receiving a beacon, the neighbor table is updated. Neighbors, for which no beacon has been received within a specified time, are removed from the table. If the MAC layer does not include a NDP, the functionality must be provided by IARP. [11]

The relationship between the components is illustrated in Fig 5.

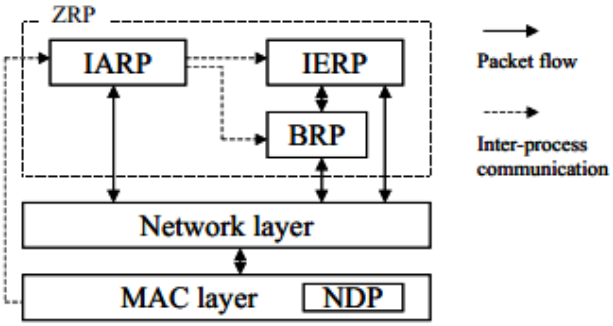

Fig. 5. ZRP architecture

OVERVIEW OF OLSR

OLSR (Optimized Link State Routing Protocol) uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths. The key concept used in the protocol is that of multipoint relays (MPRs). Each node selects a set of its neighbor nodes as MPRs. Only nodes selected as MPRs are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs thus provide an efficient mechanism for flooding control traffic by reducing the number of re- transmissions required.

IV. ENERGY AWARE ZOLSR- IDS SCHEME

After we may see that ZRP scheme subdivides the networks and forwards the packet based on zones,

By adopting this ZRP routing protocol with along OLSR energy consumption of nodes is drastically reduced

Our algorithm step is as follows

1. Intially apply ZRP protocol and have the number of zones count i.
2. For each zones choose MRPs. Nodes selected as MPRs also have a special responsibility when declaring link state information in the network. Indeed, the only requirement for OLSR to provide shortest path routes to all destinations is that MPR nodes declare link- state information for their MPR selectors. Nodes that have been selected as multipoint relays by some neighbor node(s) announce this information periodically in their control messages.Thereby a node announces to the network that it has reachability to the nodes which have selected it as an MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the network.

3. Here EAACK approach is used to find the IDSand Table.

Because of dynamic nature of MANETS, and minimum energy, with OLSR theme combined EAACK.

V. CONCLUSION

The Security and Energy are always a potential issue in MANETs, a system which provides high throughput and packet delivery in a secured manner is designed. In the proposed system, the malicious attacks are efficiently detected with minimum energy. Since the transmission power and average delay of each node is considered periodically for rout discovery with OLSR it avoids the chances to cut the network and assures faster packet transmission.

The proposed system focus mainly combining the theme of 2 routing protocols and combining its best feature for detecting the intruder with minimum energy. With this approach we planned to reduce the traffic overhead caused by the two protocols.

REFERENCES

[1] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[2] I.S. Jacobs T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Se*New York: Springer- Verlag, 2008.

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

[4] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[5] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[6] N. Kang, E. Shakshuki, and T. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs," *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, March 2013.

[7] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf. Perform., Comput., Commun.*, 2004, pp. 747–752.

[8] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in *Proc. Radio Wireless Conf.*, 2003, pp. 75–78.

[9] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[10] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.

[11] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks, June 2001, IETF Internet Draft, draft-ietf-manet-brp-01.txt