Intrusion Detection System of Mobile AdHoc Network based on Extension Techniques of Watchdog

G.Girija[1], Dr.M.G.Sumithra[2], G.Brindha[3], Gowdhami.N[4]
PG scholar, Bannari Amman Institute of Technology[1, 4]
Professor, Dept. of ECE , Bannari Amman Institute of Technology[2]
Assistant Professor, Dept. of ECE, Muthayammal Engineering college[3]

ABSTRACT
Mobile Ad-hoc network is widely used as emerging technology in many applications. It is also vulnerable to various network layer attacks, because of its network architecture and its routing protocol. Watchdog is the widely used intrusion detection system. Recently, several schemes have been introduced to overcome the limitations of watchdog which results in additional packet overhead in the network. The proposed scheme is based on clustering approach and it effectively detects the shortcomings of watchdog namely limited transmission range, receiver collision, false misbehavior report and collusion problem. About 37% decrease in the end to end delay is achieved when proposed method is used in the network. The security level of the network is further enhanced by the use of Diffie-Hellman key agreement algorithm.

Keyword:
MANET, Intrusion Detection System, Network layer attacks, Watchdog, Diffie-Hellman key agreement algorithm.

1. INTRODUCTION
Mobile Ad-Hoc Network [13] consists of group of mobile nodes communicating with each other without a fixed infrastructure. Since the nodes are free to move the topology of the network may change often and there is a greater probability for intruders to easily enter the network and they performs various network layer attacks [6] on the network. MANETs are envisioned to support advanced applications such as military operations (formations of soldiers, tanks, planes), civil applications (e.g. audio and video conferencing, sport events, telemetric applications), disaster situations (e.g., earthquakes, fires, floods), and integration with cellular systems. Several routing protocols are proposed to find a efficient path between the source and destination in the network. Sometimes, malicious node enters the network and becomes a part of the routing path. After joining the network, the intruder performs various types of attack on the network and degrades the network performance. A secure routing protocol for MANET should satisfy the following requirements [14],

- Confidentiality
- Integrity
- Non-repudiation
- Availability

Intrusion Detection System (IDS) [4] is used to detect the presence of malicious node in the network. If a particular node is detected as malicious node, then the IDS removes the malicious node from the routing table thereby preventing the network from further attack. Intrusion Detection system [8] [11] is used to detect the presence of malicious node in the network and to prevent the malicious node from performing further attacks on the network.

2. RELATED WORK
The following section describes the various intrusion detection system used in the MANET. Anoosha Prathapani [2] proposed a novel strategy by employing mobile honeypot agents that utilize their topological knowledge and detect such spurious route advertisements. They are deployed as roaming software agents that tour the network and lure attackers by sending route request advertisements. The valuable information on attacker's strategy is collected from the intrusion logs gathered at a given honeypot. Gunhee Lee et al. [3] proposed a clustering based approach to mitigate DoS attack in the network. The cluster head maintains a list of its one hop and two hop neighbors. The number of packets sent to the other nodes, the number of packets forwarded by the nodes and number of packets transmitted by the nodes present within the cluster is maintained in a table at the cluster head. Based on the table content, the malicious nodes that are present in a network can be found. Liu et al [7] proposed the TWOACK scheme that overcomes the Limited transmission range and receiver collision problem. In this technique, for every 3 consecutive nodes found in the network the third node takes the responsibility of sending the acknowledgement packet to the first node. Since number of acknowledgement packets are exchanged, it results in increased network overhead. Based on TWOACK, Sheltami et al. [5] proposed a new scheme named AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which may be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called Acknowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. Marti et al and giuli [1] proposed the watchdog intrusion detection system to identify the malicious node present in the network and to improve the overall throughput performance of the network. Once the malicious node is identified in the network Path rater [12] is used to remove that particular misbehaving node from the routing table thereby preventing the further attacks. Watchdog suffers from the following six weaknesses 1) Receiver collision 2) false misbehavior report 3) Limited transmission range 4) Ambiguous collision 5) collusion and 6) partial dropping. Though it suffers from the above shortcomings, it is widely used.

3. PROPOSED WORK

The proposed intrusion detection system is based on the clustering approach. The legitimate node in the network is chosen as the cluster head. Then, the selected cluster head monitors the nodes that are present within the cluster and detects the presence of malicious node in the network. The following phases are involved in the proposed method:

- Cluster formation and table maintenance phase.
- Transmission phase and table updation.
- Detection of false misbehavior report and limited transmission range.
- Detection of receiver collision and collusion problem.

3.1 Cluster Formation and Table Maintenance Phase

In this phase a list of one-hop neighbors and two-hop neighbors are discovered by the cluster node. A number of trusted legitimate nodes present in the network are elected as a cluster head in the network. After being elected, cluster head sends a packet to its selected neighbor and collects information about its neighbor and stores the collected information in a table. The cluster head should have the high transmission range to cover its neighbors effectively. Once the neighbor node is discovered, the cluster head creates a table and maintains information about the nodes in its table for further verification. If a node is a neighbor of two cluster heads, it joins the cluster with cluster head that is closer in distance. In addition to this each neighboring header periodically transmits the control information that contains its identity and the maximum time that a packet takes to propagate between the neighboring clusters. This control information is stored in a table. The Maximum propagation time is stored in a NACK timer.

Once the cluster formation is completed, the cluster head creates a table that contains information about its one-hop and two-hop neighbors. If a new node wants to join the cluster, it should register its identity with the cluster head. Once the registration is over, the entry for that particular node is created in the table. The cluster formation is shown below in the figure 1.

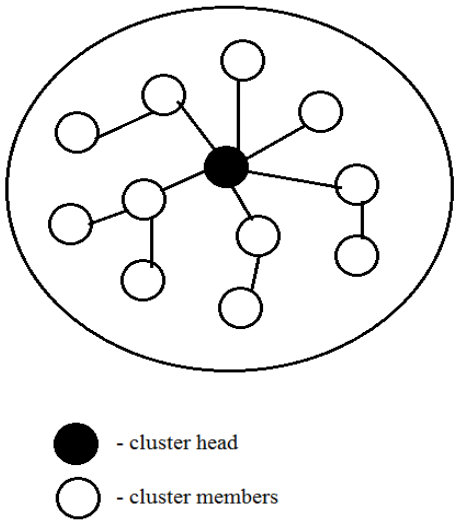

Figure 1 Cluster formation

3.2 Transmission Phase and the Table Updation Process

Any node that wishes to transmit data, initiates the route discovery process. The discovered route includes all the cluster head of the clusters that are found in the path and its cluster members. If the packet is not received within a particular timeout period specified by the NACK timer, negative acknowledgement is send back to the cluster head of the previous cluster. The packets will be stored in the buffer at each cluster head for the time specified by the NACK timer. When the receiver node receives the data packet, it sends back a acknowledgement packet to the cluster head of its preceding cluster and it propagates along the reverse path to the sender. Since Diffie-Hellman key agreement algorithm [9][10] is used, the cluster members cannot read or modify the content of the acknowledgement packet. It is read only by the cluster heads. In this way, the acknowledgement packet is sent to the sender node in a secured manner. Through the route discovery process, each cluster head knows that it is a part of the route and forwards the packet effectively in the transmission phase.

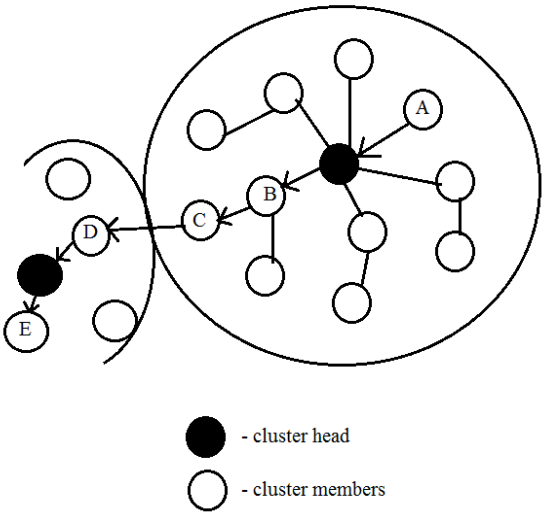

Figure 2 Route discovery and transmission process

In the figure 2, the route discovery and transmission process is shown. In figure 1, Node A found in cluster 1 wishes to transmit packet to the node E that is present in the cluster 2. The route from source to the destination includes the cluster head from both the clusters. The route request packet contains the receiver identity and the total number of packets involved in the current transmission. Similarly, the route reply packet contains the source identity and the total number of packets involved in the current transmission. The cluster head makes entry about the current transmission information in its routing table.

3.3 Detection of False Misbehavior Report and Limited Transmission Range

If any intruder is present in the network, this phase detects the presence of the intruder and removes that particular node from the network. In false misbehavior report problem, the intruder falsely reports the legal node as malicious ad removes that particular node from the network. The proposed method easily finds out the false misbehavior problem in MANET. If the misbehavior report is generated, the cluster head waits for a time period specified in NACK timer. If the reported malicious node really drops the packet without forwarding, the NACK packet is received at the cluster head. Else, if the

report is false NACK packet will not be received at the cluster head. From this, the cluster head learns whether the malicious report is true or false. In the case of limited transmission range problem, the NACK packet is received at the cluster head. In the above two cases, a new path is found between the two cluster head and the packet is transmitted.

3.4 Detection of Receiver Collision and Collusion Problem

If the packet is not forwarded because of the receiver collision, NACK packet will be received at the cluster head and the malicious activity present in the network is detected. Since the routing path includes cluster head and one or two of its cluster member, if two nodes compromises to impose collusion problem on the network, it is detected easily by the cluster head. Hence, the proposed method easily finds out the receiver collision and collusion problem of watchdog.

4. SIMULATION RESULTS

Network simulator-2 is used for the simulation. The simulation scenario consists of about 100 nodes and area 1000 × 1000 m.

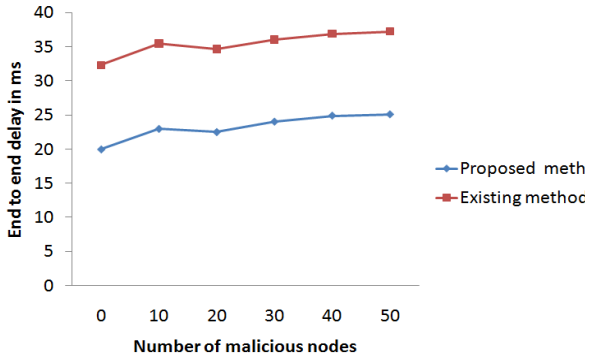

Figure 3 End to End delay

About 50% of malicious node is considered for the experiment. Figure 3 shows the graph obtained for End to End delay analyses. When the number of malicious nodes present in the network is increased, the delay increases. In the existing EAACK scheme, MRA phase is used to detect the false misbehavior report. In this phase alternate route is found to the source in order to detect the false misbehavior report. In the proposed scheme, alternate route is discovered only between the two adjacent cluster heads in order to detect the false misbehavior report problem. Hence, network delay is reduced in the proposed method when compared with the existing method.

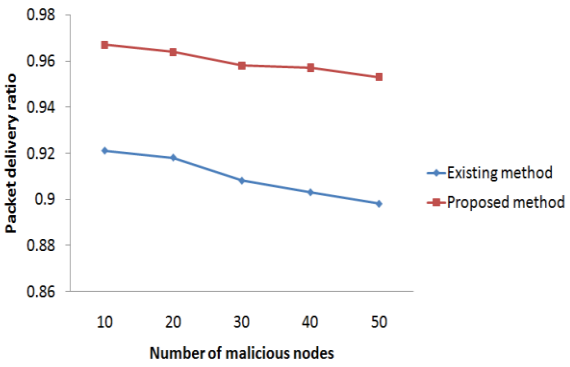

Figure 4 Packet delivery ratios

Figure 4 shows the simulation results obtained for packet delivery ratio parameter. Since the proposed method effectively eliminates the collusion problem of watchdog, it achieves higher packet delivery ratio.

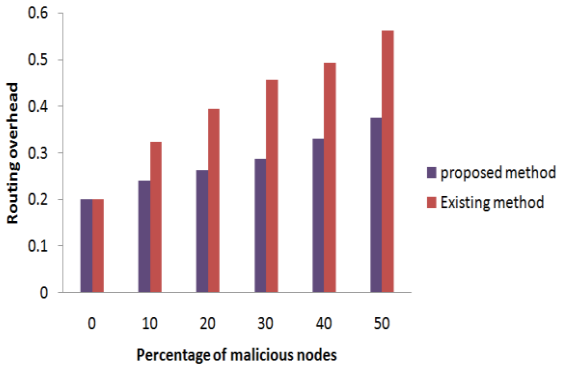

Figure 5 Routing overhead

The simulation result for routing overhead is shown in the figure 5. In the existing technique, since the alternate route is found between the source and destination, it involves transmission of multiple route request and reply packet and this introduces additional overhead in the network.

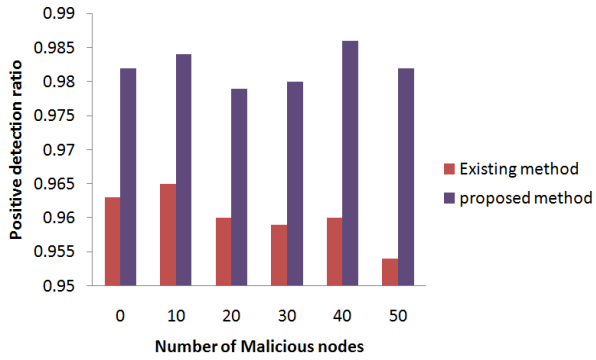

Figure 6 Positive detection ratios

Fig. 6 shows the positive detection ratio obtained for the existing and the proposed method. In the EAACK technique, because of collusion problem the nodes in the network fail to detect the presence of malicious node in the network. Since these problems are eliminated in the proposed method the positive detection ratio obtained is of higher values when compared with the existing watchdog technique

5. CONCLUSION

The proposed scheme effectively detects the shortcomings of watchdog namely limited transmission range, receiver collision, false misbehavior report and collusion problem and prevents the malicious node from taking part in further network activities. The proposed scheme increases the packet delivery ratio and the routing overhead is reduced. In addition to this, packet transmission is highly secured because of the use of Diffie-Hellman key agreement algorithm. About 37% decrease in end to end delay is achieved when proposed method is used in the network. Since it effectively detects the shortcomings of watchdog it resulted in higher positive detection ratio. In future, some additional mechanism can be implemented in the proposed technique to detect the other limitations of watchdog. Some other cryptographic technique may be implemented to provide additional security to the system.

6. REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE transactions on industrial electronics, vol. 60, no. 3, March 2013

[2] Anoosha Prathapani · Lakshmi Santhanam · Dharma P. Agrawal "Detection of blackhole attack in aWireless Mesh Network using intelligent honeypot agents", in springer 2013

[3] Gunhee Lee , Wonil Kim, Kangseok Kim, Sangyoon Oh and Dong-kyoo Kim, "An approach to mitigate DoS attack based on routing misbehavior in wireless ad hoc networks", in springer 2013

[4] Adnan Nadeem and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", in the proceedings of IEEE communications surveys & tutorials, March 2013

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

[6] Anantvalee T and Wu J "A Survey on Intrusion Detection in Mobile Ad Hoc Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008

[7] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5,pp. 536–550, May 2007.

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

[9] R. Rivest, A. Shamir, and L. Adleman "A method for obtaining digital signatures and public-key cryptosystems" Commun, ACM, vol. 21, no. 2, pp. 120–126, Feb. 1999.

[10] Olivier Chevassut, Emmanuel Bresson and David Pointcheval, "On intrusion detection and response for mobile ad hoc networks," in Proceedings of IEEE International Conference on Computing, Communication., 2004, pp. 747–752.

[11] Hu Y, Perrig A, and Johnson D, Packet Leashes "A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", in Proceedings of IEEE INFOCOM, 2002.

[12] Mamatha G.S and Sharma S.C, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", International Journal of Computer Applications, vol. 9– No.9, November 2010

[13] Srinivasan T, Mahadevan V, Meyyappan A, Manikandan A, Nivedita and M,Pavithra N, "Hybrid Agents for Power Aware Intrusion Detection in Highly Mobile Ad-hoc networks", proceedings of International Conference on Systems and Network Communication (ICSNC'06) October 2006.

[14] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Ariadne - A secure On-Demand routing protocol for Ad hoc networks"; Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, pp. 12-23, 2002.