RESEARCH ARTICLE OPEN ACCESS

Intrusion Detection in Wireless Sensor Networks: A Proposal To Recover From Breach

[1]Sumanpreet Kaur and Mahendra Kumar[2]
[1]Research Scholar Guru Kashi University, Talwandi Sabo, Bathinda, India
sumankaurpreet@yahoo.com
[2]Professor, D.R.(Research), Guru Kashi University, Talwandi Sabo, Bathinda, India

ABSTRACT
WSNs architectures are infra-structure-less network with high degree of flexibility. Security is major concern in this ad-hoc network. This is the prime area of interest for research scholars. This paper proposes a new algorithm for recovering from intruder and is based on AODV protocol. The attack from hacker is considered as direct or active. The proposed algorithm helps in repairing the loss. Using this scheme various metrics used for adhoc network are taken care of viz packet delivery ratio, throughput and average delay produced.

KEYWORD: MANET,WSNs, AODV, Intrusion, Security, Intrusion Detection System (IDS)

Date of Submission: 18-10-2021 Date of Acceptance: 02-11-2021

I. INTRODUCTION

In a network that is established for special needs and is of strategic nature, that needs attention from the security point of view too. This network needs special attention, the connected devices many a time need to perform dual role or need to perform multiple duties, like being sender receiver; work as router and work as supervisor of the network too. In this free environment, security is of prime concern [3,4]. Protocols can be implemented for prevention like encryption and authentication techniques or/and intrusion detection system (IDS). Two types of IDS are there; anomaly based IDS and misuse based IDS [2]. The normal node profile is taken into consideration in anomaly based system and unexpected behaviour of node in considered as intrusion [4]. In misuse base system, the activities of the node are matched with activities of other nodes in the network. The activities themselves show the unexpected behaviour. In case both activities are going on in the network, it is defined hybrid IDS. It is obvious that the attackers are intelligent enough to intrude into the network. It is the responsibility of the IDS to detect the malicious node and remove it from the network. There are two types of protocols used in MANET categorised as proactive and reactive routing protocols. The present manuscript discusses reactive routing protocol methodology in adhoc demand distance vector (AODV) [13, 15]. The route discovery phase uses route request (RREQ) and route reply (RREP) packets to discover the route from source to destination and route maintenance phase uses HELLO packet and route error (RERR) packet in order to maintain the route and inform about the error.

II. LITERATURE SURVEY

In the literature survey various IDS are discussed underlying protocols, architecture and types of attacks. The four types of IDS architectures namely standalone; distributed & collaborative; hierarchical; and mobile agent IDS are taken into consideration here. The wireless networks can be configured in multi layered or flat network infrastructure. The later is suitable for the civil type of activities as all nodes have equal responsibility in the routing protocol. In the former case the nodes are organised in clusters, a cluster head is designated to centralize the routing operations amongst clusters and is used in strategic emergency or war like situations.

DSR bases confidant approach is similar to overcome the drawbacks of the watchdog and path-rater scheme by ignoring misbehaving nodes as a remedial process in the routing process [8]. The nodes identify neighbouring nodes as friends and enemies on the basis of trust. The trusted friends are informed of enemies. This approach claims the packet delivery ratio very high (more than 97%). This approach degrades the throughput of clients and servers. **CONFIDANT(2002)** [8][14].

Ocean is another extension to the DSR protocol, a monitoring and a reputation system is employed through it. The protocol uses second hand reputation messages to avoid phantom intrusion detections. This approach can detect misbehaving and selfish nodes. But, the detection efficiency decreases with the increase in the density of misbehaving nodes. The simulation results show that at high threshold values, other second hand protocols perform better in high mobility of the nodes. The Ocean is very sensitive to change of the threshold parameters, while second hand protocols are more consistent over varying threshold limits. This is not quite effective in penalizing misleading nodes **OCEAN(2003)** [11][14].

Scan is based on two central ideas that are: each node monitors its neighbours for routing/packet forwarding misbehaviour independently; observing neighbours by cross validating the overhead traffic with other nodes. The nodes are declared malicious by a majority decision. This assumes that the network density is sufficiently high. The network services are temporarily halted during intrusion detection in this protocol. The assumption that network density is high may not always hold. Increase in mobility results in higher false positives. Besides, the packet delivery ratio can be heavily affected in the interval during which an attack is launched and when it is detected. **SCAN(2006)** [9][14].

A cluster based IDSX solution is used as an extended architecture. In a simulation based experiment, the results showed that the IDSX solution does not give any false positives. The anomaly based on IDS is deployed at the first line of defence and dirty packet forwarding is handled. This approach works in the pre-set boundaries [5]. This approach is feasible and practical enough in adhoc networks but some of these may also be considered as the limiting constraints. This approach of IDSX has not been compared with any of the IDS solutions. Also, the proposed two-step approach would make the task of IDS expensive in terms of energy and resource consumption **IDSX(2007)**[5, 14].

Another approach uses the unsupervised learning concept in Artificial Neural Networks (ANN) using with self-organizing maps using AODV. This technique is named as eSOM, it uses U-matrix to represent data classes. Those regions which represented malicious information are watermarked with block-wise method using the lattice method. As a new attack is launched it causes changes in the pixel values [14]. The watermarking technique can identify if any pixel has been modified. This makes it very sensitive towards detecting intrusions. The solution is considerably efficient and remains consistent with variations in mobility. This approach needs to be trained in regular time periods, there are additional overhead and thus energy efficiency decreases in this algorithm **Neural Network and Watermarking Technique(2007)[6]**.

The IDS in MANET based on the Vicky, Clarke and Groves (VCG) model requires every node to be as honest as possible. The leaders those participate honestly are elected that result in optimal resource utilization. The experimental results indicate VCG model performs well during leader election by producing a higher percentage of alive nodes. It shows that the normal nodes carry out more duty of intrusion detection and die faster as the number of selfish nodes increases. The selfish nodes do not exhaust energy to run the IDS service, the percentage of packet analysis decreases with time. In the case of static scenarios, the model elects the same node as leader repeatedly. This causes the normal nodes to die very fast **A leader election model(2008)[7]**.

In another approach namely HIDS is based on trust values of the nodes. It dynamically increase/ decrease depending on its behaviour: node with normal behaviour is positively rewarded; malicious activity results in negative rewards for that node. The trust on a node is recomputed based on its current honesty rate, and the rewards that it has earned. A comparative study between SCAN and HIDS shows that the latter involves lower storage and communicational overhead than SCAN. HIDS is inherently protected against false positives. However, maintaining up-to-date tables at different nodes, as required by HIDS, may not be an energy-efficient strategy. Also the proposed HIDS offers only a generic architecture for secure route detection **HIDS(2008)** [10][14].

A hybrid solution combines the watchdog and path-rater scheme as neither SCAN nor Watchdog and Path-raters address the mobility issue that well. The hybrid solution also suffers from this problem. There can be no fixed nodes to behave as supervisor. As this results in increased overhead along with energy consumption as sometimes supervisor nodes themselves can become malicious. To detect Denial of Service (DoS) attacks, the criteria for attack detection cannot be so rigid. Also, the history of a node that had being behaving normal, should be taken in to consideration before writing it off as malicious as soon as it deviates from normal behaviour **hybrid solution(2010)** Marti et al[9].

PROPOSED PLAN

The AODV routing protocol, a modified algorithm is designed and changes has been made for the repairing phase. It carries out local repair using time to live (TTL). This scheme makes changes in its repair mechanism. The route request (RREQ) phase and route reply (RREP) phase are same as in AODV. The route repair mechanism of AODV protocol has been modified in two phases as explained here. In first phase the intruder is detected using sequence number policy. In second phase an algorithm is used to bypass the intruder and select a new path to carryout recovery of damage done by intruder. The figure 1(a) shows the normal routing process of AODV protocol whereas the route has been established between source node S and destination node D. It follows normal route request and reply phase using RREQ and RREP packet. The network consists of 9 nodes from sequence numbers 1 to 9.

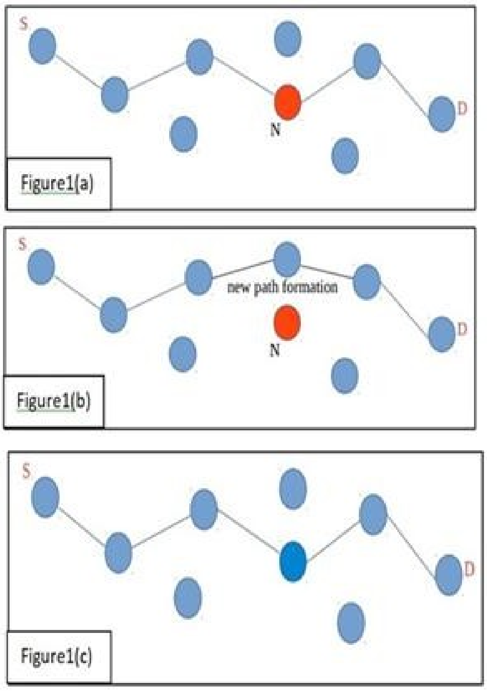


Figure 1: All states of nodes in pictorial form

Phase I: Intruder Detection

- Nodes check route-table
- After reply phase, sequence numbers are checked after each beacon
- If a particular sequence number is out of sequence/out of range, the node is treated as intruder

The figure 1(b) explains how proposed algorithm detects the intruder during route recovery phase of AODV protocol. Here the node N shown in red colour is detected as false node or malafide node as its sequence number is found out of range in the MANET where valid sequence numbers are from 1 to 9.

Phase II: Repairing the intruder

- Makes changes in RREQ in routing table.
- A new route request is sent from node that is one hop back the intruder node (n to n-1).
- Then from node n-1, a new path is created and intruder is isolated or bypassed.

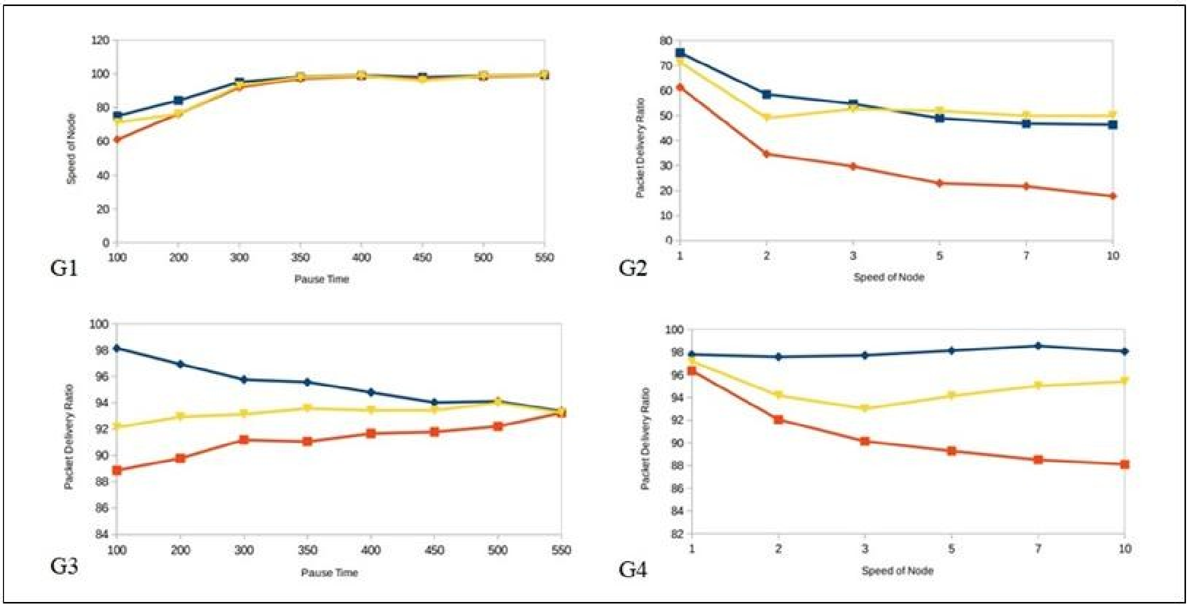
The figure 1(c) shows that the intruder node has been isolated and removed from the network and a new path as shown by different colour line has been created by the previous node from the intruder node N. Thus the network has been recovered by the proposed algorithm.

The performance of algorithm is checked using various metrics for mobile adhoc networks like packet delivery ratio, throughput and average-delay. The proposed algorithm is executed in NS2 simulator for small, medium and large network scenario taking 10, 20 and 50 nodes respectively. Pause time in ms and speed of node in ms are taken as the parameter to check the results of different metrics. The result section includes the graphs that show the performance of the modified algorithm.

III. RESULTS

The graphs have been used to describe the results obtained from the execution of proposed plan. Each graph displays three scenarios of AODV routing protocol namely normal (in blue colour), after the intrusion (in red colour) when intruder enters the scene and creates havoc and then after the network is being repaired using the proposed algorithm is shown in yellow colour.

The graph G1 gives the description of 10 nodes scenario with pause time as a function in three different scenes. The pause time varies from 100 ms to 550 ms. If the intruder does not disturb the network to the larger extent the situation is not critical, but it has been shown using red notation. The proposed scheme takes care of intruder it either bypasses or removes it. The results show that the proposed scheme has been able to modify the results in positive direction as displayed by yellow line. A few more cases have been taken with 20 and 50 nodes. The graph G2 is representation of PDR with speed as a function for 10 nodes in three scenes of AODV routing protocol. The speed has been varied from 1 ms to 10 ms. The normal scenario is shown in blue line notation and red line notation denotes entry of an intruder. The yellow line is depiction of recovery from intruder as proposed by new scheme. As desired the proposed scheme is able to take care of PDR and is reaching the target at almost normal scene. As shown the increase of 25% to 65% is a great recovery particularly at higher speed of 10ms. The graph G3 shows the execution of AODV protocol in MANET of 50 nodes for varying pause time from 100 ms to 550 ms. It depicts the major reduction in packet delivery ratio caused by malicious node as blue line is at comparatively much higher value than red line. The increased traffic may be the reason for intruder to affect the performance of neighbouring nodes. In case of 10 nodes this situation is not critical as the traffic is very less. After applying the proposed algorithm to repair the false or malicious node considerable improvement in packet delivery ratio has been achieved shown in graph by yellow notation. This shows the proposed algorithm is working well to improve the performance of AODV protocol as the network becomes denser.



Graph A: Representation of all states

The graph G4 is representation of PDR with speed as a function for 50 nodes in three scenes of AODV routing protocol. Speed has been varied from 1 ms to 10 ms. Normal scenario is blue line notation and red line notation denotes entry of an intruder. Yellow line is depiction of recovery from intruder as proposed by new scheme. As desired the proposed scheme is able overcome the loss introduced by the intruder or malicious node and recover the PDR which is very close to normal profile of the network. The graph displays that as the speed of node increases the normal PDR reaching upto 98% and intruder reduces it to 88% which is recovered by the proposed scheme upto 96% is a significant gain.

IV. CONCLUSION

The paper is a detailed study of AODV with three views as normal, with intruder and repair. The repair has been done in second phase of the AODV . The Local Route repair has been modified and various metrics has been used to verify the scheme. Two parameters as Speed and Pause time has been used with various scenes as 10, 20 and 50 nodes. The new scheme has been able to repair the existing scheme and results are shown using graphs. The whole work has been conducted using NS2 and using various scenarios with Random way Point Model. More work will be conducted for other protocols also including DSR and TORA. The effect of fading will also be considered and more emphasis will be on use of stable routes.

REFERENCES

[1]. Deb N., Chakraborty M, Chaki N., "The evolution of IDS Solutions in Wireless Adhoc Networks to Wireless Mesh Network",IJNSA vol 3, no. 6, November 2011.

[2]. Solanke J. G., Chandra P.R., "Literature Survey on IDS in MANET", IJSET, vol. 4,issue 1, January 2015, ISSSN 2278-7798

[3]. Kush A., Seema "Evaluation of Routing Schemes for MANET" in A. Mantri et al. (Eds.): HPAGC 2011, CCIS 169, pp. 575–580, 2011**.** © Springer-Verlag Berlin Heidelberg 2011.

[4]. Kush A., Divya, Vishal ," Energy efficient Routing for MANET" , Intl conf on applied and communication tech, Elsevier Pub, pp 189-194., 2014.

[5]. Chaki R., Chaki N.; "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network", Proceedings of the IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2007.

[6]. Mitrokotsa A., Komninos N., Douligeris C., "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," International Conference on Pervasive Services, pp. 118-127, IEEE Int'l Conference on Pervasive Services, 2007.

[7]. Mohammed N., Otrok H., Wang L., Debbabi M., Bhattacharya P., Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

[8]. Buchegger S. and Boudec J. Le, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, 2002.

[9]. Yang H., Shu J., Meng X., Lu S., "SCAN: self-organized network-layer security in mobile ad hoc networks," IEEE J. on Sel. Areas in Communications, vol. 24, pp. 261-273, 2006.

[10]. Sil P., Chaki R., Chaki N.; "HIDS: Honesty-rate based collaborative Intrusion Detection System for Mobile Ad-Hoc Networks", Proc. of 7th IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2008.

[11]. Bansal S. and Baker M., "Observation-Based Cooperation Enforcement in Ad hoc Networks," Research Report cs.NI/0307012, Stanford University, 2003.

[12]. Kathirvel A., Enhanced Triple Umpiring System for Security and Performance Improvement in Wireless MANETS, International Journal of Communication Networks and Information Security (IJCNIS), Vol 2, No 2 (2010).

[13]. Hinds A., Ngulube M., Zhu S., and Hussain Al-Aqrabi,"A Review of Routing Protocols for Mobile Adhoc Networks",International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[14]. Kulkarni A., Prashant R. P., Agrawal M., "Literature Survey on IDS of MANET", International Journal of scientific research and management (IJSRM) , volume3,issue9,Pages3549-3552, 2015, www.ijsrm.in ISSN (e): 2321-3418.

[15]. Taneja S., Kush D. A. and Makkar A. (2011), "End to End Analysis of Prominent on Demand Routing protocols" ,International Journal of Computer Science and technology, vol. II, no. 1, pp. 42-46.