Accurate Detection of Multi-layer Packet Dropping Attacks Using Distributed Mobile Agents in MANET

1MythiliBoopathi and 2R.Seetha

1Assistant Professor (SG), School of Information Technology and Engineering, VIT University, mythilibaopathiphd@gmail.com
2Assistant Professor(Sr), School of Information Technology and Engineering, VIT University, rseetha@vit.ac.in

Abstract: Detecting multi-layer packet drop attacks may result in extraordinary computational overhead in Mobile Ad Hoc Networks (MANET). Most of the existing works consider only data packet drop ignoring the routing packets drops. In this paper, a technique for accurate detection of malicious multi-layer packet drop attacks using mobile agents (MPDDMA) is proposed. In this technique, mobile agents are deployed in each node to detect selective dropping of routing and data packets by the malicious nodes. The source node identities the nodes whose route request and route reply count significantly differs from others by a margin. Similarly, the source node identifies the nodes whose packet received count significantly differs from others by another margin. The source then applies Fuzzy logic decision model with these margin values and MAC layer packet drop value as input variables and returns the output as probability of maliciousness (PrM). Experimental results show that MPDDMA technique achieves better detection accuracy and reduced packet drops.

Keywords: MANET; Multi-layer; Attacks; Mobile Agent; MAC

1. Introduction

MANET is an independent architecture of movable nodes which form a wireless network. In MANETs, the network topology may vary fast and randomly [1]. They are beneficial in presentation zones like tragedy managing crisis and saving processes where it is not at all likely to have definite set-up. MANETs are categorised by its inordinate suppleness. On the other hand, MANET’s characteristic susceptibility upsurges their safety perils. Though MANETs are naturally active and supportive, it requires effectual and actual safety contrivances to protect the movable nodes. Interruption discovery and deterrence are main contrivances to lessen probable interruptions [2]. Because of the absence of approval amenities, it is tough to notice hateful nodes. In MANET, nodes may be battery-powered and may have very inadequate capitals that may do the usage of heavy-weight safety explanations disagreeable [3]. As the procedure of observation of nodes needs to be reiterated across numerous hops along a track, it experiences enormous communication overhead. Furthermore, midway observation nodes flop to notice the choosy tumbling bout [12].

Attack detection is a major concern of computer safety. It provides protection contrary to computer usage after physical, verification and admission control [4]. The old-fashioned method of defending wired/wireless systems with firewalls and encryption software is not adequate [5]. Because of the little sensing speediness and great incorrect optimistic amount of old-fashioned discovery methods, a novel design centred on movable means [6] have been industrialised. The Intellectual and movable features of the representative are chief benefits of using movable representatives[15].
There are three types of selective packet dropping attacks in MANET. In first type, the misbehaviour nodes may not forward the routing packets. In second type of attack, data packets may not be forwarded at the time of data delivery. In third type of attack, both routing and data packets may not be forwarded[16].

1.1 Problem Identification and Objectives

The Intelligent agent based IDS using multiclass SVM [2], the agent based IDS architecture [10] and the distributed mobile agent based IDS [11], need datasets for detecting DoS attacks only. Since it has a pre-processing phase, it consumes more time and results in high computational overhead. Moreover, it did not handle the misbehaviour attacks like packet dropping.

The MADSN [3] approach considers the packet drops only at the routing layer. But packet drops may occur at MAC layer also. Moreover, until the MA visits the malicious node, the packet drop attack could not be detected. The mobile agent based IDS [4] assumes the cluster heads are honest, which may not be true in all the cases. Though the Fuzzy based detection system [7] categorizes the attacker levels, it did not present the detailed methodology for detecting various attacks. The anomaly detection system (ADS) [8] has focused on malicious nodes which affect the routing process only, ignoring the data forwarding phase. The intelligent authorization agent [12] approach did not present any standard technique for detecting the packet dropping attacks.

In [9], by analyzing the correlations between lost packets, the packet losses can be distinguished as because of link failures or attacks. But it considers only data packet drop ignoring the routing packets.

Based on the above identified problems, the main goals of this work are listed as follows:

- To consider the packet drop at network and MAC layers
- To consider both routing and data packets forwarding
- To distinguish between regular packet drop or malicious drops
- To detection technique should consume minimum time and involve less overhead

2. Related Works

Ganapathy et al [2] have described a novel intellectual agent-based interference discovery prototype for MANET by means of a mixture of characteristic choice, outlier discovery, and improved multiclass SVM organisation means. For this cause, an effectual pre-processing method is suggested that advances the discovery exactness and decreases the dispensation period. Furthermore, two novel procedures, viz., an Intellectual Instrument Biased Expanse Outlier Discovery procedure and an Intellectual Agent-based Improved Multiclass Provision Vector Machine procedure are planned for sensing the interlopers in a dispersed record atmosphere that practices intellectual means for faith organisation and synchronization in business dealing.

Binod Kumar Pattanayak et al [4] have presented mobile agent centred intrusion recognition and defence design for a collected MANET. Mobile agent exists in every group and every group runs a precise solicitation at any time. This solicitation’s precise method marks the network healthier to exterior interruptions focussed at the nodes.

SHANTHI et al [7] have suggested a joint method called fuzzy centred interruption recognition and group centred genuine direction-finding. This method includes the recognition of assailant level of the nodes in network layers using fuzzy logic method. The conviction worth of every node is rationalised based on the perceived assailant level. When basic node needs to transfer a data package to the terminus, the path with dependable nodes is nominated by means of group based ant colony optimization (ACO) method.

Vikram Narayandas et al [8] have offered system for detecting a malevolent node in a group centred MANET. It uses AODV protocol that achieves track detection and data progressing. In a group centred
topology a verge is smeared to look if this core response numeral is more than the verge cost. If so the node is malevolent. Then every node directs awareness to its group head and its nearby nodes. The planned ADS eludes the routing to a malevolent node thus averting high dynamic depletion of the linked nodes and defence the data transmission in the MANET.

Tao Shu et al [9] have established a homomorphic linear authenticator (HLA) centred communal reviewing design which permits the sensor to check the openness of the package loss info conveyed by nodes. This structure is secrecy conserving, complicity resilient, and experiences small communication and stowage overheads. To decrease the calculation overhead of the standard system, a technique is also proposed, which permits one to employ recognition exactness for inferior calculation intricacy.

Sameh et al [10] have suggested a mediator centred interruption recognition and deterrence scheme has been intended by means of ant colony procedure. Every node is supervised by means of a movable mediator of the network and every node turns a precise solicitation. Multi Depot packet routing (MDPR) is used to examine the packets from numerous nodes. Support vector machines (SVM) is utilised to recognize the malevolent actions of present package with canned actions.

Maad Kamal Al-Anmi [11] have established the signature-based IDS method in a MANET by applying the rear broadcast procedure. As a result, the sign of malevolent actions or unwanted actions are frequently predicted and competently reckoned by augmenting the parametric arrangement of rear broadcast procedure at the time of investigational outcomes. This empirically exposes its efficiency for the proportion of recognition table up to 98.6 percentage.

Aranganathan et al [12] have suggested a scheme by means of Intelligent Authorized Agent based Detection (IAAD) for the sensing tenacity. The projected approval mediator centred scheme effectively implemented authentic nodes in the networks with enhanced presentation metrics of package transfer proportion, package loss degree, endwise suspension and output in contrary to malevolent nodes in mobile adhoc networks.

Basant Subba et al [13] have suggested a novel cross IDS system that includes a verge based frivolous unit and a influential variance based tough component. The frivolous component computes the Packet Forwarding Rate (PFR) of the possible malevolent nodes. The interruption discovery procedure was demonstrated as a multi-stage Bayesian game amid the group head and the possible malevolent node, to trigger the tough component.

Yu Zhang et al [14] have established an Audit-based Misbehavior Detection (AMD) mechanism for sensing and dividing package dipping bouts. AMD puts together repute based path detection and misconduct recognition. The status managing scheme guesses the features of nodes by reviewing.

### 3. Multi-layer Packet Dropping attack detection using Distributed Mobile Agents (MPDDMA)

#### 3.1 Brief Description of work

This work aims to design a technique for accurate detection of malicious multi-layer packet dropping attacks using mobile agents. In this work, mobile agents are deployed in each node to detect the selective drop attack of routing and data packets. During route determination phase, source node identifies the nodes whose count significantly differs from others. Similarly, during data transmission phase, source node identifies the nodes whose count significantly differs from others based on the MAC layer packet drop value. Then source applies Fuzzy logic decision model which margin values and MAC layer packet drop value as input variables and returns the output probability of maliciousness (PrM) is returned as the output.

By checking the value of (PrM) the malicious nodes are confirmed and categorized as follows:

- Dropping only routing packets
3.2 Estimation of Metrics

3.2.1 Packet Delivery Ratio

It is termed as the proportions of package onward stand to the package obtain stand.

\[ \text{PDR} = \frac{C_f}{C_r} \]  

(1)

The path with the least delay and high delivery probability is selected as the route for data transmission.

3.2.2 Packet Drop Rate

The packet error rate (PER) is given by

\[ \text{PER} = \frac{1}{1 + (w_n \rho)^v_n} \quad \forall \rho \geq 0 \]  

(2)

Where \( v_n \) and \( w_n \) are factors depending on AMC mode and packet size

Where \( \rho \) - (SINR)

The packet loss rate (PDropMAC) is termed as the amount of data packages which are not efficiently transferred to the terminus.

\[ \text{PER}(\rho) = \text{PDrop}_{\text{MAC}} \left( \frac{1}{(\lambda' - 1)} \right) \]  

(3)

3.3 Neighbor Setup Phase

This phase is explained as follows:

1. Initially mobile agents (MA) are deployed in each node to detect the selective dropping of routing and data packets from the malicious nodes.

2. MA broadcasts a HELLO message with source and destination node ID, hop count and PDR (estimated in section 3.2.1) to the one hop neighbours nodes.

| Table -1 HELLO message |
|-------------------------|
| Source Node ID | Destination Node ID | Hop Count | PDR |

3. The receiver stores the neighbour information in the following table

| Table – 2 Neighbour Table |
|---------------------------|
| NID | One hop neighbour | Hop Count | Packet Delivery Ratio |

4. Then the receiver sends response message to the sender.
5. By repeating the same process, all the nodes build their neighbour table.

3.4 Route Discovery Phase

Let RFV be the route forward verification message

Let VR be the verification reply message.

The route discovery phase can be explained as below

- The source \( S \) broadcasts the RREQ packets to its one-hop and two-hop neighbourhoods towards the destination \( D \):

\[
S \xrightarrow{\text{RREQ}} N_j \xrightarrow{\text{RREQ}} D
\]

- Each MA\(_j\) at intermediate node \( N_j \) counts the number of RREQs received (NO\(_{\text{RREQ}}\)) from \( N_j \).
- Similarly, it counts the number of RREPs (NO\(_{\text{RREP}}\)) received at \( N_j \) from \( N_{j+1}\).
- Once \( S \) receives the RREPs from various paths, it broadcasts a RFV message to all mobile agents and waits for a time period of \( T_{\text{req}} \) seconds.
- Within \( T_{\text{req}} \), each MA\(_j\) replies back the VR which contains the NO\(_{\text{RREQ}}\) and NO\(_{\text{RREP}}\) at \( N_j \).
- \( S \) then aggregates the replies and analyzes them by cross checking the replies from various agents.
- \( S \) then identifies the nodes whose count significantly differs from others by a margin \( \delta_1 \).

3.5 Data Transmission Phase

The data transmission phase can be explained as below

1. MAs at each node estimate the MAC layer packet drops \( \text{PDrop}_{\text{MAC}} \) (estimated in section 3.2.2) by determining the channel condition and contention.
2. Similar to Route Discovery phase,

- Within \( T_{\text{req}} \), each MA\(_j\) replies back the VR which contains the NO\(_{\text{RREQ}}\) and NO\(_{\text{RREP}}\) at \( N_j \).
- \( S \) then aggregates the replies and analyzes them by cross checking the replies from various agents.
- \( S \) then identifies the nodes whose count significantly differs from others by a margin \( \delta_2 \).

3.6 Fuzzy Logic Decision (FLD)

The Fuzzy logic decision model is applied by \( S \) which considers \( \delta_1 \), \( \delta_2 \) and \( \text{PDrop}_{\text{MAC}} \) as input variables. By applying the fuzzy rules, the output probability of maliciousness (PrM) is returned as the output. FLD architecture consists of four major divisions specifically Fuzzification, Rule generation, Inference System and Defuzzification. The FLD model is shown in Figure 1.
The fuzzy logic uses three input variables and one output variable. This involves fuzzification of input variables $\delta_1$ (A), $\delta_2$ (B), $P_{Drop_{MAC}}$ (C) into fuzzy sets. The linguistic functions for the input are: (H) High and (L) Low. The Fuzzy output variable Degree of Maliciousness (D) can be as (H) High, (M) Medium and (L) Low.

The Fuzz sets and membership function for the input and output variables are shown in Figure 2 to 5. The triangular fuzzy sets are utilized in the membership functions, since they are commonly utilized in most of the applications.

Figure 2 Membership Function of Margin $\delta_1$
Figure 3 Membership Function of Margin $\delta^2$

Figure 4 Membership Function of MAC Layer Packet Drop

Figure 5 Membership Function of Degree of Maliciousness

Table 1 shows the table of fuzzy rules table which comprises of 8 rules.
Table 1 Fuzzy Rules table

| Rule No | Margin (A) | Margin (B) | MAC Layer Packet Drop (C) | Degree of Maliciousness (D) |
|---------|------------|------------|----------------------------|-----------------------------|
| 1       | Low        | Low        | Low                        | Low                         |
| 2       | Low        | Low        | High                       | Low                         |
| 3       | Low        | High       | Low                        | Low                         |
| 4       | Low        | High       | High                       | Medium                      |
| 5       | High       | Low        | Low                        | Low                         |
| 6       | High       | Low        | High                       | Medium                      |
| 7       | High       | High       | Low                        | Medium                      |
| 8       | High       | High       | High                       | High                        |

From Table 1, the following inference rules can be observed:

Rule 8.
If (A, B and C = High)

Then
Output Probability of Maliciousness is high
Malicious Nodes drops both routing and data packets

End if

Rule 6
If (A = high) (C = High)

Then
Output Probability of Maliciousness is Medium
Malicious Nodes drops routing packets

End if

Thus, by checking the value of (PrM) the malicious nodes are confirmed and categorized as follows:
- Dropping only routing packets
- Dropping only data packets
- Dropping both routing and data packets

The centroid of area method is used for defuzzification, which is given by the following equation:

\[
F_{QoS} = \frac{\int \eta_{agg}(F) \, df}{\eta_{agg}(F)_{df}}
\]  

(4)

Where \( \eta_{agg}(F) \) = aggregated output of membership function

4. Experimental Evaluation

4.1 Experimental Parameters
The MPDDMA scheme has been implemented in NS2. It is compared with the Privacy Preserving Truthful detection (PPTD) of packet dropping attacks [9]. The metrics detection delay, packet drop, packet delivery ratio and detection accuracy are measured. The simulation parameters are listed in Table 2.

| Number of nodes | 50          |
|-----------------|-------------|
| Topology size   | 1000m X 1000m |
| MAC Protocol    | IEEE 802.11 |
| Traffic model   | CBR         |
| Number of malicious nodes | 2 to 10     |
| Packet size     | 1000 bytes  |

Table 2 Simulation parameters

4.2 Results and Description

The performance results of varying the number of misbehaving nodes, launching data packet and routing packet drop attacks, are varied from 2 to 10.

Figure 5 shows the detection delay for both the techniques. It shows that the E2D of MPDDMA increases from 0.2 to 1.2 seconds and the E2D of PPTD decreases from 3.8 to 1.7 seconds. Ultimately, the delay of MPDDMA is 61% of lesser than PPTD.
Figure 6 Packet Delivery Ratio of varying attackers

Figure 6 shows the packet delivery ratio for both the techniques. It shows that PDR of MPDDMA varies from 0.99 to 0.36 and the PDR of PPTD varies from 0.28 to 0.21. So the PDR of MPDDMA is 52% of higher than PPTD.

Figure 7 Total packets dropped for varying attackers

The graph showing the results of Packet drop for varying the attackers is shown in figure 7. The figure depicts that the drop of MPDDMA increases in the range of 2 to 453 and the drop of PPTD increases in the range of 795 to 1760.Ultimately, the packet drop of MPDDMA is 80% of lesser than PPTD.
Figure 8 shows the detection accuracy for varying attackers. It shows that detection accuracy of MPDDMA varies from 594 to 1925 and the detection accuracy of PPTD varies from 1209 to 2925. Hence, the detection accuracy of MPDDMA is 34% of lesser than PPTD.

5. Conclusion

The technique of Multi-layer Packet Dropping attack detection using Distributed Mobile Agents has been proposed in this paper. In this work, mobile agents are deployed in each node to detect the selective dropping of routing and data packets. The source node applies Fuzzy logic decision model which margin values and MAC layer packet drop value as input variables and returns the output probability of maliciousness is returned as the output. Performance comparison results indicate that the proposed MPDDMA technique increases the detection accuracy thereby reducing the number of packet drops and detection delay.

References

1. Mojtaba Karami, Marjan Kuchaki Rafsanjani, Amir Hosein Fathi Navid and Yaeghoob Yavari, "QAIDS: Quantitative and Agent based Intrusion Detection System", Computer and Information Science Vol. 4, No. 2; March 2011.
2. S. Ganapathy, P. Yogesh, and A. Kannan, "Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM", Computational Intelligence and Neuroscience, Volume 2012, Article ID 850259, 10 pages.
3. Debudutta Barman Roy and Rituparna Chaki, "MADSN: Mobile Agent Based Detection of Selfish Node in MANET", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.
4. Binod Kumar Pattanayak and Mamata Rath, "A MOBILE AGENT BASED INTRUSION DETECTION SYSTEM ARCHITECTURE FOR MOBILE AD HOC NETWORKS", Journal of Computer Science 10 (6): 970-975, 2014.
5. R. Nakkeeran, T. Aruldoss Albert and R. Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks", IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.
6. YOUSEF EL MOURABIT, AHMED TOUMANARI, HICHAM ZOUGAGH, "A Mobile Agent Approach for IDS in Mobile Ad Hoc Network", IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 1, No 1, January 2014.
7. K. SHANTHI and T. JEBARAJAN, "FUZZY BASED DETECTION AND SWARM BASED AUTHENTICATED ROUTING IN MANET", Journal of Theoretical and Applied Information Technology, Vol. 63 No.3, 2014.
8. Vikram Narayandas, Sujanavan Tiruwayipati, Madasu Hanmandlu and Lakshmi Thimmareddy, "Anomaly Detection System in a Cluster Based MANET", Springer, Computer Communication, Networking and Internet Security, Lecture Notes in Networks and Systems 5, DOI 10.1007/978-981-10-3226-4_2, 2017.
9. Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 4, APRIL 2015.
10. S. Sampath and V. Thiagarasu, "An Agent based Intrusion Detection System Architecture for Mobile Ad Hoc Networks using Ant Colony Algorithm", International Journal of Engineering Research & Technology (IJERT), Vol. 4 Issue 07, July-2015.
11. Maad Kamal Al-anni, "A Distributed Mobile Agent based on Intrusion Detection System for MANET", International Journal of Computer and Information Engineering, Vol-11, No-6, 2017.
12. A. Aranganathan and C.D. Suriyakala, "Detection of Malicious Nodes using Intelligent Authorization Agent for Clustering in MANETs", International Journal of Control Theory and Applications, Vol-10, No-30, 2017.
13. Basant Subba, Santosh Biswas and Sushanta Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation", An International Journal on Engineering Science and Technology, Elsevier 19, 782–799, 2016.
14. Yu Zhang, Loukas Lazos and William Jr. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, Volume: 15, Issue: 8, 2016.
15. Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., & Thong, P. H. (2018). APD-JFAD: accurate prevention and detection of jelly fish attack in MANET. Ieee Access, 6, 56954-56965.
16. Suseendran, G., Chandrasekar, E., & Nayyar, A. (2019). Defending jellyfish attack in mobile ad hoc networks via novel fuzzy system rule. In Data Management, Analytics and Innovation (pp. 437-455). Springer, Singapore.
17. Natarajan, B., Obaidat, M.S., Sadoun, B., Manoharan, R., Ramachandran, S. and Velusamy, N., 2020. New Clustering-Based Semantic Service Selection and User Preferential Model. IEEE Systems Journal. DOI: 10.1109/JSYST.2020.3025407.
18. Nataraj, S.K., Al-Turjman, F., Adom, A.H., Sitharthan, R., Rajesh, M. and Kumar, R., 2020. Intelligent Robotic Chair with Thought Control and Communication Aid Using Higher Order Spectra Band Features. IEEE Sensors Journal, DOI: 10.1109/JSEN.2020.3020971.
19. Babu, R.G., Obaidat, M.S., Amudha, V., Manoharan, R. and Sitharthan, R., 2020. Comparative analysis of distributive linear and non-linear optimised spectrum sensing clustering techniques in cognitive radio network systems. IET Networks, DOI: 10.1049/iet-net.2020.0122.