Efficient Intrusion detection of malicious node using Bayesian Hybrid Detection in MANET

Sangeetha. V1, Vaneeta M2, S Swapna Kumar3, Piyush Kumar Pareek4, Sunanda Dixit5
1Associate Professor, Dept of ISE, Sai Vidya Institute of Technology, Bengaluru
2Associate Professor, Dept of CSE, K.S. Institute of Technology, Bengaluru
3Professor, Dept of E &C, Vidya Academy of Science & Technology, Thrissur
4Professor, Dept of CSE, East West College of Engineering, Bengaluru
5Associate Professor, Dept of CSE, BMSIT & M, Bengaluru

Abstract. In the past several years there have been considerable interest developed towards study on distributed networks. The key underlying application under such technology is mobile ad hoc networks (MANETs), which have been exploiting the range of research opportunity. In MANET due to infrastructure less network and dynamic topology changes, security becomes one of the important issues. The defense strategies such as intrusion detection system (IDS) impose a method to build efficient detection of malicious nodes. Game theory is mainly used to study security problems identification in MANET. The Bayesian Hybrid Detection (BHD) is applied to detect the malicious nodes. A BHD allows the defender to adjust based on opponent observation. The simulation is carried out using the MATLAB for malicious nodes detection. The security degree is measured by the payoff index and system stability index (SSI). Also the processing vs. accuracy index level is measured to identify reliability of detection. The proposed system enables for enhancing security in MANET’s by modeling the interactions among a malicious node with number of legitimate nodes. This is suitable for future works on multilayer security problem in MANET.

Keywords: Bayesian game, Cluster nodes, Game theory, Intrusions, genetic algorithms

1. Introduction

In the wireless networking the nodes are spatially and randomly distributed, leads to exploration field of mobile ad hoc networks (MANETs). MANET is a network that consist of set of mobile nodes that communicate each other over wireless link. These mobile nodes will always establish dynamically own network without any infrastructure to forward data in a multi-hop mode. In a MANET, each mobile node can separately organize and interconnect with each other over bandwidth uncomfortable wireless relatives where, safety has become one of the important issues. Some of the applications in
MANETs are for military applications, disaster relief, localization measurement, digital conference so on [1].

Some of the applications of MANET are on Tactical networks, Sensor networks, Commercial environment, Educational applications, Entertainment, Localization etc. Most of the application covers the distributed mobile computing, particularly for military and defense purpose. MANET is a network constitute of mobile node that change dynamically. In MANET primary requirement is to establish a communication links among nodes. But due to infrastructure less network and dynamic topology changes, security becomes one of the important issues. There are various network security threats that exist in network, such as black hole, denial of service, grey hole, resource consumption, location disclosure, wormhole, host impersonation, information disclosure etc. [2],[3].So the flexibility and adaptability of the mobile nodes is difficult to achieve without proper monitoring in the sporadic nature of connectivity. There are few distinct characteristics of MANETs are node mobility, resource constraints, due to these unique characteristic it makes the network vulnerable to a variety of attacks forms[4].

Game theory deals with the study of network security problems, which can be used for node identification in MANET. Game theory has been extensively used in different types of networks as tool to model a variety of problems to design the mobile communication network systems. The applications of game theory, is basically a noncooperative and cooperative game theory used for minimization of energy, random access and power control in wireless networks [8].

In game theory two players provides security correlation between attacker and a defender. The interaction between an attacker and defender produce a two different player such as non-cooperative non-zero-sum game. The intrusion detection approach is applied to cluster for monitoring the behavior of the nodes. The Bayesian Hybrid Detection (BHD) is applied to detect the malicious nodes [9]. A BHD allows the defender to adjust based on opponent observation. The strategic modeling is applied to detect the ambiguity of cluster nodes vulnerability. Thereby this reduces the malicious nodes by improving the reliability in detection. To monitor the efficiency of the improvement initially the cost function, system stability index (SSI) is the robustness of the detection systems to malicious nodes in the distributed network. Also the processing vs. accuracy index level measures reliability of detection.

The paper is organized as follows. Section 2 includes the existing literature survey. Section 3 discusses about the proposed architecture and optimization method. Section 4 discusses about result analysis. Finally, the whole work is concluded in Section 5.

2. Literature Survey
The research work in IDS’s proposed by Anderson et al., shows the models for intrusion detection for wired networks [10]. This approach uses the knowledge that is most domains specific to build suitable detection systems.

Otrok et al., address the problem that deals with increasing the intrusions within a cluster of nodes in ad hoc networks [11]. To reduce the issues that arise in IDS, a selected node called leader node is usually elected to handle the intrusion within the entire cluster. However, in many methods cluster solutions will always elect a leader randomly without considering the resource level of nodes that cause the node to die faster. Network is also vulnerable to many such selfish nodes that will not provide services to others while at the same time benefiting from such services. Yanwei et al., proposed the another Game Theoretic approach called Mean Field for optimizing the security issues in Mobile adhoc Network [12]. This approach will use a mathematical tool to solve the many security issues in MANET. In Mean Field Game theoretic approach, the mobile nodes can be alerted to make strategic security defense decision without centralized administration.
Wei Sun et al., worked on energy efficient neighbor discovery method in MANET and Wireless sensor Network (WSN) [13]. The paper mainly focused on minimum power consumption method for neighbor discovery. This cause most of packet drops in density networks in worst case. Perrig et al., proposed asymmetric cryptographic algorithms that is suitable for providing security in WSN. This scheme does not produce maximum reliability and security on data security for all types of wireless sensor networks [14]. Wang et al., proposed the study towards secure routing protocol was that used the mechanism to strengthen the communication system in MANET [19]. The mechanism found to be resistive against malicious behaviour of the mobile nodes. However, such method lack due to weak processing strategies.

The proposed system thereby addresses all issues that can aim at modeling situations in which strategic decision have to make for specific actions. To improve monitoring strategies that maximize the utility of a defending node, which is comprised of both security values and energy resources game theory, is applied. A game theory is a powerful tool to study the security problem in mobile networks. However, the efficient optimization game theory is applied to security by considering two players in the security game model: an attacker and a defender for a network with distributed administration.

The next section discusses about a novel technique where these issues are addressed using game theory. In this technique, we propose a novel Bayesian Hybrid Detection (BDH) game theoretic approach with efficient cost function for security in MANETs.

3. Proposed System design

The main purpose of the intrusion detection system is to formulate a energy efficient intrusion detection that can easily identify vulnerable behavior of the mobile host nodes in mobile adhoc network. The clusters consist of different region of mobility of mobile node as shown in Figure 1.

![Figure 1: Cluster distribution mechanism](image)

The MANET consists of multiple clusters, where a huge number of mobile host nodes reside inside the cluster. The MANET is always an infrastructure less network and nodes within cluster are heterogeneous. Network can consist of Normal node, malicious node and Selfish node. Each node in mobile adhoc network are extremely decentralized in nature, hence, it is also very decisive to ascertain security. The main purpose of the proposed system is to study the malicious behavior of node. Inside network, there are different ranges of attacks in adhoc networks, so one solution of Intrusion detection system will not be possible to cater up the security requirements. The flowchart of the proposed system is as shown in Figure 2.
The main purpose is to develop a system that uses game theory approach based on ‘Bayesian Hybrid Detection (BDH)’, here the different vulnerable and the most susceptible behavior of the malicious nodes is probabilistically evaluated. The proposed model will apply the BDH approach as shown in Figure 2. The main work of the proposed paper is as follow:

1. To select the energy efficient node by applying an efficient algorithms and apply game theory.
2. The intrusion detection approach is applied to cluster for regulating the behavior of the mobile nodes.
3. To use a strategic modeling approaches that can reduce the ambiguity of vulnerability and can easily detect the intrusion in the systems.
4. To identifying and reduce the malicious mobile nodes in order to increase the reliability in detection.
5. To verify the performance of proposed system to existing techniques.

Figure 2 shows the BDH flow framework of the cluster architecture, that shows that a simulation study under adversarial node.
Figure 3: BDH framework

Here Mobile nodes are classified into three different types like Normal nodes, malicious nodes, and selfish nodes respectively. For energy efficient nodes and to control energy spent on IDS, the BDH analyze on low and high IDS. The updated system is implemented using the genetic algorithm.

According to Liu et.al (2005a) the BDH system applies high IDS system. These two IDS monitor the maliciousness using two players (Attacker and Defender). Whenever there occurs any deviation from the normal node behavior that it is considered as an anomaly behaviour.

In the MANET the nodes are mobile, thereby the cost function such as BW, packet size and CPU power consumption are linearly formulated. A dynamic changing mobility pattern of the node applies the strategic decision considering the rules for different patterns. The proposed model applies optimality on efficient clustering nodes using genetic algorithm and intrusion detection optimization using BDH.

3.1. Efficient distributed nodes

\[
\text{Cost}_E = F(C_{PE}, S_{WE}, P_{CE}, B_{WE}) \tag{1}
\]

where, \(C_{PE}\) is encoded data computation, \(S_{WE}\) is the traffic switching, \(P_{CE}\) is power consumption, \(B_{WE}\) is bandwidth and \(E\) is the index range from 1 to \(n\) for number of nodes.

The cost function \(F = \sum_1^\delta \varphi_E\) \tag{2} 

where, \(\delta\) is the number of cost parameter of different cost functions from equation 1, \((C_{PE}, S_{WE}, P_{CE}, B_{WE})\) are expressed as follow:

The computational cost can be formulated as:

\[
\varphi_{Cp}(E) = c_{Cp} \frac{P_E}{P(t)} \tag{3}
\]

where, \(P_E\) is total packet size to be transmitted, \(P(t)\) already sent at time \(t\), \(c_{Cp}\) is the bandwidth cost coefficient per capacity unit.

The switching cost can be expressed as:

\[
\varphi_{Sw}(E) = c_{Sw}[1 + f_E(E_x, E_w)] \tag{4}
\]
where, \( E_c \) is the current encryption algorithm, \( E_x \) is the next encryption algorithm of sensor node that applies the condition as:

\[
f_E(E_x, E_w) = \begin{cases} 0; & E_c = E_x \\ 1; & E_c \neq E_x \end{cases}
\]

The power consumption cost \( \varphi_{Pw} \) is fixed as threshold level coefficient such as:

\[
\varphi_{Pw}(E) = c_{Pw}
\]

The bandwidth cost rate \( \varphi_{Bw} \) is expressed as:

\[
\varphi_{Bw}(E) = c_{Pw}
\]

where, \( C_E \) is considered as the total capacity of the channel of the network and \( C(t) \) is the remaining capacity of channel at time \( t \).

3.2. Intrusion Detection

The cluster network node that is received efficiently from previous method is given as an input to BDH framework. The attacker (i) has two conditions: Attack and Non-attack. The defender (j) has two condition: Monitor and non-monitor. We modeled the attack/defender game as two ‘Bayesian Hybrid Detection’.

Monitor is a defender collects data from energy efficient network and examines the data with IDS. The following condition is considered for the strategy form of Game theory.

\[
\begin{align*}
\text{Attack-Monitor: } & (1 - 2\beta)\gamma - C_a(2\beta - 1)\gamma - C_m \\
\text{Attack-Not-monitor: } & \gamma - C_a, -\gamma \\
\text{Not-attack-Monitor: } & 0, a\gamma - C_m \\
\text{Not-attack-Not-monitor: } & 0, 0
\end{align*}
\]

The \( C_a \) and \( C_m \) denote the costs of attacking and monitoring, \( \gamma \) represent a security loss, payoff matrix \( \beta \) represent the detection rate and \( \gamma \) represent the false alarm.

If \( C_a > 0 \) and \( C_m > 0 \); then it is for monitor and attack.

If \( \gamma > C_a \) and \( \gamma > C_m \); then it is for no monitor and defeat to attack.

The objective of attack and defender is to maximize their pay-off function that depends on Attacker and Monitor probability \( p^* \) and \( q^* \) is given by:

\[
p^* = \frac{a\gamma + C_m}{(2\beta + a)\gamma}
\]

\[
q^* = \frac{\gamma - C_a}{2\beta\gamma}
\]

The IDS has the advantage to identify attack source (s). Let \( p \) be the probability of Attacker (i) and \( q \) the probability of defender (j).
The expected payoff of defender (j) as Monitor is given as:

\[ E_u(j \text{Monitor}) = p^* \mu_0 ((2\beta - 1)\gamma - C_m) - (1 - p^*) \mu_0 (\alpha \gamma - C_m) - (1 - \mu_0) (\alpha \gamma - C_m) \]  

(10)

The expected payoff of defender (j) as Not-monitor is given as:

\[ E_u(j \text{Not-monitor}) = q^* \mu_0 \gamma \]  

(11)

3.3. Intrusion detection Optimization

The cluster of intrusion detection node when applied to Back testing Classification model will provide the good stability and model ranking. The system stability index (SSI) calculated as follows:

\[ SSI = \sum_{i=1}^{k} (\text{observed}_i - \text{expected}_i) \cdot \ln \frac{\text{observed}_i}{\text{expected}_i} \]  

(12)

The use of HRD framework reduces the probability of false alarm. A random mobility pattern of the node applies the strategic decision to multi-layer intrusion detection system using multi-stage games. The next section discusses about the implementation strategy.

4. Result Analysis

The simulation is carried out using the MATLAB for malicious nodes detection. The security degree is measured by the payoff index. To monitor the efficiency of the improvement initially the cost function is calculated to check the performance of proposed system to existing techniques. The system stability index (SSI) is calculated to verify the robustness of the detection systems with respect to malicious nodes in the distributed network. Also the processing vs. accuracy index level is measured to identify reliability of detection.

Here mainly we will discuss the results obtained from the proposed study. In the proposed system we implement game theory approach, which is used decision making theory; the final trace of separate types of security of nodes is shown in Figure 4.

![Figure 4: Distribution of nodes concentrations](image)

The intrusion Attacker detection using game theory for an efficient BHD system shows percentage of distribution up to 24 numbers of game stages shown in Figure 5.
Under the BHD algorithm the defender nodes success percentage is closer to attacker percentage of success identification of malicious nodes under three classes shown in Figure 6.

The processing time taken for BDH system is efficient that shows higher reliability in the intrusion detection. The proposed system considers accuracy in detection rate and also processing time in the three types of nodes environment shown in Figure 7.

The proposed approach introduced by [16] has obtained good accuracy by incorporating to state-based transition rules in the game theory approach, considering all the mobile nodes. Hence we can say this system is more or less recursive. But system lacks to address multiple attacker issues, which is addressed in another approach called ZIDS that incorporated the monitoring system for coordination.
system among the mobile attacker nodes. Hence the proposed system can be applied the cost function as well as BHD system for the measurement of SSI. Therefore, the computational time for Wang et al. [16] approach is quite complex and high as compared to other two approaches.

5. Conclusion
Security issues are one of the core problems in mobile ad hoc networks owing to the decentralized architecture. The proposed system introduces a new scheme that can acts as multi-layer security under two different stages. The many existing system has already considered various IDS system against particular type of attacks in MANET. However, few different types of attacking strategies which succeed any firewall system can be able to detect using this technique. Therefore, the IDS based on the malicious behavior of the mobile nodes in the simulation area, can detect against multiple forms of attacks.

The system enhances security in MANET’s by modelling the different interactions among a malicious node and with a number of legitimate nodes. This is suitable for future works on multilayer security problem in MANET.

References
[1] Lima M, Santos A, Pujolle G, “A survey of survivability in Mobile Ad Hoc Networks”, (2019), IEEE. Communications surv. tutor, 11(1): 66-77
[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, (Feb. 2014), “Security in mobile ad hoc networks: challenges and solutions”, IEEE Trans. Wireless Commun., vol. 11, pp. 38–47.
[3] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, “Joint topology control and authentication design in mobile ad hoc networks with cooperative communications”, (July 2012), IEEE Trans. Veh. Technol., vol. 61, no. 6, pp. 2674–2685.
[4] Y. Wang, F. Yu, H. Tang, and M. Huang, “A mean field game theoretic approach for security enhancements in mobile ad hoc networks”, (Mar 2014), IEEE Trans. Wireless Communication, vol. 13, pp. 1616–1627
[5] Zhang Y, Lee W, “Intrusion Detection in Wireless Ad Hoc Networks”, (2020), Proceeding of the 6th Annual Int. Conf. on Mobile Computing and Networking (ACM MobiCom’00) held at Boston, pp. 275-283.
[6] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, “Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks”, (Sept.2018), IEEE Trans. Wireless Commun., vol. 10, no. 9, pp. 3064–3073.
[7] Liu, J., F.R. Yu, C.H. Lung and H. Tang, “Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks”, (2019), IEEE Trans.Wireless Commun., 8(2): page 806-815.
[8] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks”, (Feb. 2014), IEEE Trans. Wireless Commun., vol. 11, no. 1, pp. 48–60.
[9] Miao X, Zhou X, Yi Wu H, “A cooperative differential game model based on transmission Rate in wireless networks”, (2019), J. Operat. Res. Lett., 38(1): 292-295.
[10] Nurmi, P., “em Modelling Routing in Wireless Ad Hoc Networks with Dynamic Bayesian Games”, Proc. (2019), First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON 2004., October, pp.63, 70.
[11] Anderson, D. Frivold, T. and Valdes, A., “Next-generation Intrusion Detection Expert System (NIDES): A Summary”, (2019), Computer Science Laboratory SRI-CSL-95-07.

[12] Otrok H, Mohammed N, Wang L, Debbabi M, Bhattacharya P, “game-theoretic intrusion detection model for Mobile Ad Hoc Networks”, (2018), J. Comput. Commun., 31(4): 708-721.

[13] Yanwei Wang F. Richard Yu, Helen Tang and Minyi Huang, “Mean Field Game Theoretic Approach for Security Enhancements in Mobile Adhoc Network”, March 2018, IEEE Transaction on Wireless Communication. Vol. 13, No.3.

[14] Wei Sun, Zheng Yang, Xinglin Zhang, Yunhao Liu, “Energy Efficient Neighbor Discovery in Mobile Ad hoc and Wireless sensor Network”, (2018), IEEE Communication survey , vol. 16 No. 3.

[15] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, “SPINS: Security Protocols for Wireless Sensor Networks”, (2018), ACM Mobile Comp. and Net.

[16] F. Wang, F. Wang, B. Huang, and L. T. Yang, “COSR: A Reputation-Based Secure Route Protocol in MANET”, (2020), EURASIP Journal on Wireless Communications and Networking.

[17] Z. Han and Y. L. Sun, “Distributed Cooperative Transmission with Unreliable and Untrustworthy Relay Channels”, (2019), Hindawi Publishing Corporation.

[18] Marchang N, Tripathi R, “A game theoretical approach for efficient deployment of intrusion detection system in Mobile Ad Hoc Networks”, (2017), Proceeding of the 15th Int. Conf. on Advanced Computing and Communications Held at Guwahati. Assam, pp. 460-464.

[19] Kuchaki RM, Aliahmadipour L, Javidi MM, “An optimal method for detecting internal and external intrusion in MANET”, (2018), Proceeding of the Int. Conf. on Future Generation Communication and Networking (FGCN 2019) held at Jeju Island. Korea. pp. 71-82.

[20] S. Swapna Kumar, Sangeetha V., “ZIDS: Zonal-based Intrusion Detection System for studying the malicious node behaviour in MANET”,(17-19 Dec. 2015), International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), IEEE Explore-ISBN 978-1-4673-9563-2, pp. 276 – 281.