Improved Selfish node Detection By AODV with Convex Optimization Approach

Sumiti[1]

Ph.d Research Scholar, MMICT & BM- MCA Department, MM (Deemed to be University), Mullana, Ambala, India

Abstract- Mobile ad-hoc networks (MANETs) have inadequate energy and improper path from source to destination. This leads to the selfish behavior of nodes and become unable to send packets In this research, an agent based improved approach is presented for detection of selfish node and to generate the attack preventive path over the network. The proposed method also used the fuzzy rules as the measure to take the decision about the selfishness of nodes. The proposed model is divided in three main work stages. In the first work stage of this model, N-random agents are distributed over the network for analysing the mobile nodes. The controller is defined for the distribution of these random nodes and their functioning. The agents are defined so that the maximum coverage over the network will be achieved. Each agent is defined in this research with specific coverage range. As the agents the distributed, they analysed the mobile nodes present in their coverage range.

Keywords- *selfish node, wsn, mobilenode random selection,Manet*

I. INTRODUCTION

Mobile network is the adhoc network without the existence of any centralized controller and provides the dynamic route formation over the network. The random movement of nodes is a good challenge for this network. The frequent change in topology and the cooperative communication in the network are affected by various predictable and unpredictable challenges. The mobile network can be established for any specialized network or applications or environments including the battlefield, operations are hostile terrain, close region based data acquisition etc. The flexibilities exist in the network topology and the environment adaption makes it possible to apply it for any application or environment. The key features of mobile network such as dynamic topology, multihop communication, external adaptation and limited resources facilitate it to integrate it with any environment or application. This kind of adaptation is also challenging in terms of security, external access to the network and maintaining network integrity [1,2]. A typical mobile network is shown in figure 1.1. The main objective of the mobile network is to provide the effective communication of data, voice, video and other forms of information in the public domain. The technology adaptation to the mobile network should be specific to the environment, application and domain. The objective of the constraint specification is based on the objective of the application. These objectives can be minimizing the communication delay, maximizing the communication throughput, enhancing the network lifetime etc. In a mobile network, various protocols exist and work at different layers for enabling the communication in the network. The routing protocols are mainly responsible for generating the effective and dynamic path over the network. There are various reactive, proactive and hybrid protocols which are later discussed in detail in chapter 3. These protocols are quite sensitive to the network distribution, bandwidth utilization, battery backup, communication metrics, route convergence etc. The access architecture and behaviour of mobile network is shown in Figure 1.2. The figure clearly shows that the network elements and hardware including base stations and mobile stations. The coverage of the base stations is shown in the form of cell. The mobile user available within the region of the cell can access various internet services for voice, video or data sharing. Different kind of internet services can be utilized by any mobile user using various applications. As the mobile devices are mobile and acts independently within the region, the multihop communication can be performed through these mobile devices. The communication constraints and the routing protocols are responsible for generating the effective route and for performing the effective communication over the network. Once the network is initiated with relative constraints, it can be adapted in public, private and opportunistic networks[3]. Various challenges associated to different forms of mobile network are provided in next section.

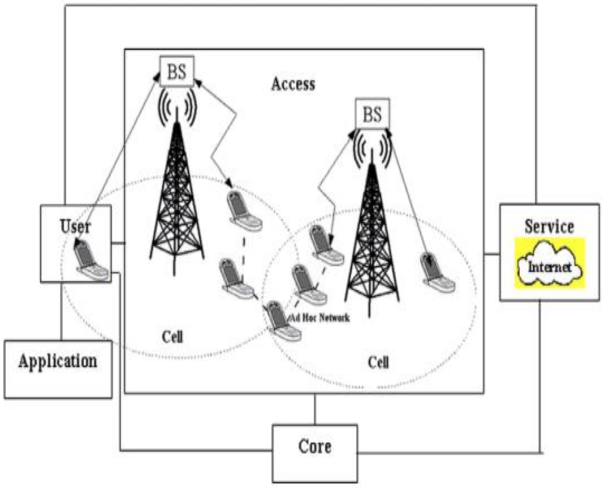

Figure 1.2 :Access Behaviour of Mobile Network[3]

1.2 Challenges in Mobile Network

The wider adaptation, dynamic nature and absence of centralized infrastructure are the most critical challenges to mobile network. The hybrid nature of the environment and the application also increases the communication complexities for the mobile network. The availability of the resources, protocol selection and environment adaptation are also the challenges faced by the mobile network[1,4,5]. Some of the common challenges that affect the performance of mobile network are listed below :

1.2.1 Security

The mobile network is the open and dynamic network which is affected by interference from internal and external nodes. The network suffers from various security lapses as each node act as the intermediate node for other communication. The man-in-middle attack is one such challenge to the network and affects the network reliability. Various security protocols and security guidelines are defined for achieving the secure and reliable communication in the network. The authentication mechanism, encoded communication are also integrated in the network for enhancing the reliability and security in the network. The security integration is adapted at different layers of mobile network and integrated with the protocols exist at different layers. The mobile network is affected by various internal and external attacks which are performed at different level and layers by different intruders. Various security mechanisms and frameworks are also available to minimize the effect of these attacks and improving the network reliability and effectiveness[4,5].

1.2. 2 Lesser Priori Trust

Mobile network is established in a public domain and in most of the application and environments, the intermediate and neighbor nodes are unknown. These unknown nodes are reason of lesser interest exist while performing the communication and deciding the forwarder node. Most of the routing algorithms or protocols use the trust as main or integrated factor to decide the next forwarder node in the network. Trust is important factor while analyzing the cooperative behaviour and contribution of possible forwarder node. The delay, neighbor interaction and packet drop ratio are the factors used to evaluate the trust for a node[6,7].

II. RELATED WORK

Szott et al.[103] provided a study on selfish node attack in two-hop IEEE 802.11 relay networks. The analytical observation was taken by the author under QoS (Quality of Service) parameter on MAC layer of the network. The topology and network environment specific complexities were also identified by the author. Author explored the effect of tamper for network traffic, source traffic and both. The effect of selfish node, its applicability and the type of attacks were discussed by the author. The attack strategies and the defense measures were also identified by the author.

Ghonge et al.[104] explored the behaviour of the network in existence of selfish node. Author provided a detailed survey on the work and improvement done for detecting the selfish node in mobile network. The drawbacks of earlier method and the new assignments defined by the author were also discussed in this paper. The audit, credit, reputation, acknowledgement and collaborative based systems provided by the researchers for detection of selfish node. Author also defined the method for route formation while detecting the selfish behaviour of nodes.

Szott et al.[105] provided a study to explore the selfish node attack respective to collaborative behaviour of nodes in 802.11s networks. The analysis was provided by the author for existing attacks as well as defined the examination behaviour for identifying new attacks in the network. The detection and prevention methods that can be approached for securing the network were also discussed in this work. The quantization method was defined for prioritizing the node behaviour respective to the attack. The cooperative behaviour of attacker nodes and their respective impact in the network was discussed in this work. The effect of attack and the parameters considered for observing the attack in MAC layer were discussed in this work. The classification of the attack and relative preventive measure were also defined in this work.

Sengathir et al.[106] provided a study on the behaviour of selfish node and defined different methods available for detection of selfish node in the network. Various reputation, context and history aware models are defined in this paper. The probabilistic reputation, conditional evaluation and history based reputation frameworks were also defined by the author for detecting the attacker node. The statistical measures were defined by author for performing the node specific analysis. The effects of selfish node on network and data transmission were also discussed in this paper. Various issues associated to the network while applying these attack detection approaches are also discussed in this paper.

Nimje et al.[107] provided a detailed study on the monitoring of selfish behaviour of nodes in mobile network and provided the detection using watchdog algorithm. Watchdog is the method that performs the pattern driven analysis for observing the complex behaviour of mobile nodes. Once the communication features of nodes are obtained, the decision rules are defined for separating the normal and the attacker nodes. The neighbor relation analysis was provided in this work for observing the malicious specific data pattern. The communication features were observed for a period for analyzing the misbehavior nodes and for identifying the normal communication. The behaviour and impact of the watchdog method was also discussed by the author.

Kodhai et al.[108] provided a study for detection of selfish node in the mobile network. The paper explored various selfish node detection methods for accurate marking of selfish node existence in the network. The node based local region analysis was provided in this work for identification of the evidence for detection of attacker node in the network. The cooperative intrusion detection methods were discussed in this paper for isolating the normal and selfish node. The work behaviour of these techniques were defined so that effective and preventive path will be generated over the network. The reputation, credit and collaborative watchdog methods were discussed and explored in this paper.

Ramya et al.[109] provided a detail study to explore the methods for improving the performance of mobile network in existence of selfish nodes. The node level participation and forwarder node criticalities were discussed in this paper. The methods were defined for detecting the selfish node and for improving the performance of the network. The methods were defined for using the individual and collaborative information within the network and locating the selfish node. Different kind of watchdog based protocols and frameworks were also explored in this paper for detection of selfish node attack.

Kumar et al.[110] provided a review on the different methods available for detection of selfish nodes in the mobile network. The method was defined for detecting and observing the network resources and the collaborative communication in the network. Watchdog, trust based, reputation based, Auction based methods were defined in this work. Some other protocols and frameworks working at different layers and features for avoiding or detecting the selfish nodes were also discussed in this proposed work. The effect and impact of these attack detection and prevention method was also defined in this paper.

Sultana et al.[111] provided a detail study of various generic and game theoretical approaches of selfish node detection and avoidance. The algorithmic methods were defined for observing the cooperation of nodes under different parameters. Different forms of game theoretical rules were formed for separating the attacker and the normal nodes in the network. The review was provided for exploring the functional behaviour of these game theoretical approaches. The cooperative characterization and rule based modeling measures were also defined in this paper. The enforcement parameters along with payoff matrix of game playing were also provided for different approaches.

Kurkure et al.[112] provided the analytical study of credit based ARAM protocol which was used for detection of selfish node in the mobile network. The method was defined for observing the infrastructural characteristics of nodes and for evaluating the dynamic behaviour of mobile nodes. The authenticated routing based communication method was discussed in this paper for enhancing the reliability in existence of selfish node attack. The comparative analysis was provided against the DSR, TORA and AODV protocols. The analysis results shows that the proposed method achieved the more accurate detection of selfish node in the mobile network and improved the network reliability.

Diarra et al.[113] provided the detailed review for observing the impact and accountability of selfish node in a mile network. Author also explored the game theory based method along with incentive driven node evaluation approach. The node based trust computation was included into his work for observing the interest and scope of the nodes. The work was defined as the multicast protocol as well as opinion routing protocol for generating the effective communication in the network. The communication behaviour features and its adaptation to the deterministic behaviour of neighbor node was also observed and monitored in this work. The finite state machine based functional behaviour was analyzed and verified in this research work.

III. THE PROPOSED METHOD

3.1 Proposed Methodology

the agent based improved method is presented for detection of selfish node in mobile network. The network level and environment specific constraints and assumptions are also defined while defining and simulating the proposed model. These constraints and assumptions are listed below:

- The nodes are distributed randomly in the network and the scalability is tested in terms of number of nodes in the network.
- The nodes in the network are defined with random mobility. The speed of the nodes is also varying.
- The source and destination nodes are also selected randomly.
- The network can have more than one selfish node and these attackers are distributed randomly.
- The proposed model is integrated and simulated with AODV protocol.
- The proposed agent based improved approach for detection of selfish node is applied on a random mobile network. The simulation of the proposed approach is done in NS2 environment. The work is simulated in three different scenarios of 49 nodes, 75 nodes and 100 nodes for achieving the scalability. The configuration parameters for these network scenarios are shown in Table 5.1. The communication and route formation in this work is done using AODV protocol. The random topology based mobile scenario is defined and the network is infected with one or more selfish nodes. The simulation and analysis results for these scenarios are provided in later sections of this chapter.
- The proposed agent based analysis approach is applied in this research for detection of selfish nodes and for generating the attack free path between the source and destination nodes. The method is defined for generating the preventive path so that the effectiveness and reliability will be improved.

Table 5.1 : Network Scenario

Properties	Value
Network Size	3000x2000 mtr
Number of Nodes	49, 75 and 100
Simulation Time	100 Sec
Protocol	AODV
Energy Model	Yes
MAC Protocol	802.11
Topology	Random
Packet size	512 Byte

IV. RESULT ANALYSIS

4.1 Result Analysis

The analytical evaluation of the proposed selfish node detection and prevention method is defined under the packet communication, packet loss, byte communication and delay parameters. The formulation of these analysis parameters is already provided in the previous sub-section. The comparative results are provided against the token based, agent based and watchdog based methods.

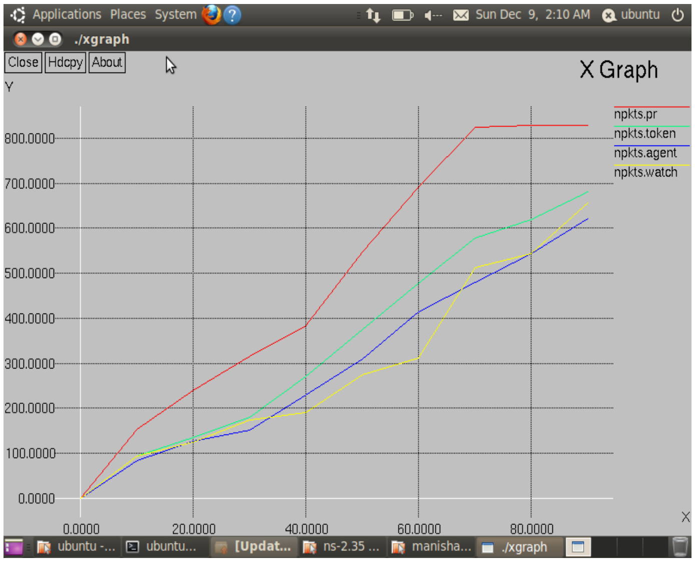

Figure 5.13: Packet Communication based Comparative Analysis

Figure 5.13 has provided the analytical evaluation of proposed selfish node detection technique against the existing methods in terms of packet transmission in the network. In this figure, x axis represents the simulation time and y axis represents the number of packets transmitted. Better the packet transmission, the reliable the communication method is considered. The line graph clearly shows that the packet communication in case of proposed method is much higher than existing methods. It clearly shows that the packet transmission and communication reliability is improved in case of proposed approach.

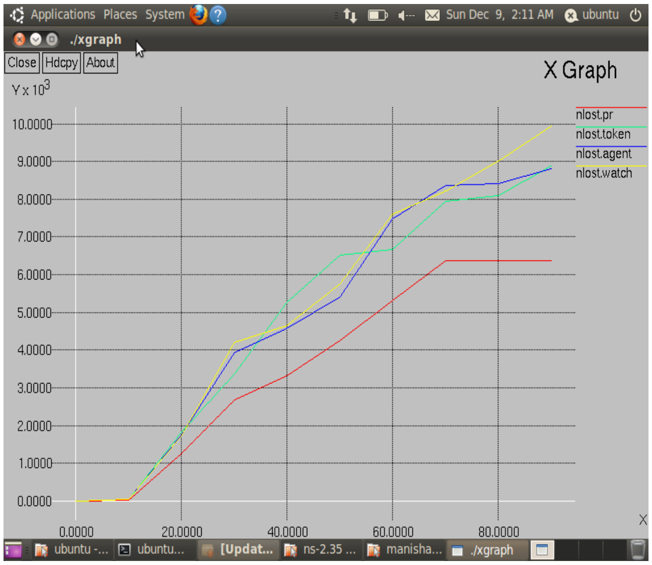

Figure 5.14: Packet Loss based Comparative Analysis

Figure 5.14 has provided the analytical evaluation of proposed selfish node detection and prevention technique against the existing methods in terms of packet loss in the network. The packet loss in a communication or routing method represents the reliability of the network. The lesser the communication loss, more effective the communication is considered. In this figure, x axis represents the simulation time and y axis represents the number of packets lost. The line graph clearly shows that the packet loss in case of proposed method is much lesser than existing methods. It clearly shows that the proposed approach identified selfish node more accurately and reduced the communication loss. The overall communication reliability of the network is improved using this proposed approach.

Figure 5.15 has provided the analytical evaluation of proposed selfish node detection and prevention technique against the existing methods in terms of packet lossrate in the network. The lossrate in a communication or routing method represents the reliability of the network. The lesser the communication loss, more effective the communication is considered. In this figure, x axis represents the simulation time and y axis represents the number of packets lossrate. The line graph clearly shows that the packet lossrate in case of proposed method is much lesser than existing methods. It clearly shows that the proposed approach identified selfish node more accurately and reduced the communication loss. The overall communication reliability of the network is improved using this proposed approach.

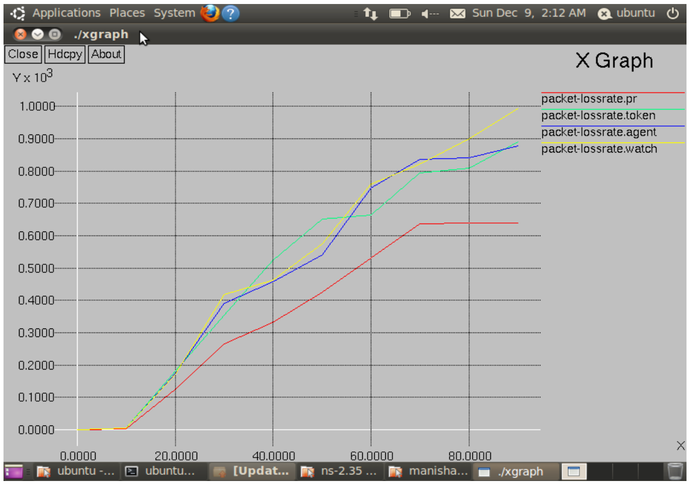

Figure 5.15: Packet Lossrate based Comparative Analysis

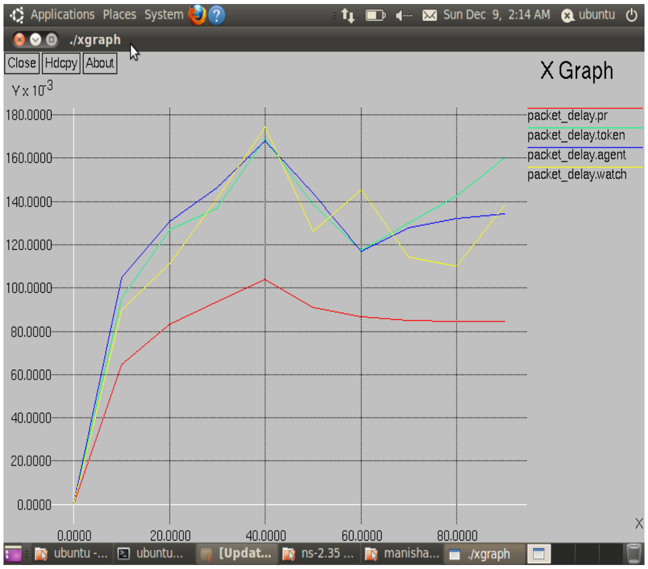

Figure 5.16 : Packet Delay based Comparative Analysis

Figure 5.16 has provided the analytical evaluation of proposed selfish node detection and prevention technique against the existing methods in terms of packet delay in the network. The packet delay in a communication or routing method represents the efficiency of the network. The lesser the communication delay, more effective the communication is considered. In this figure, x axis represents the simulation time and y axis represents the number of packets delay. The line graph clearly shows that the packet delay in case of proposed method is much lesser than existing methods. It clearly shows that the proposed approach identified selfish node more effectively and reduced the delivery time in the network. The overall efficiency of the network is improved using this proposed approach.

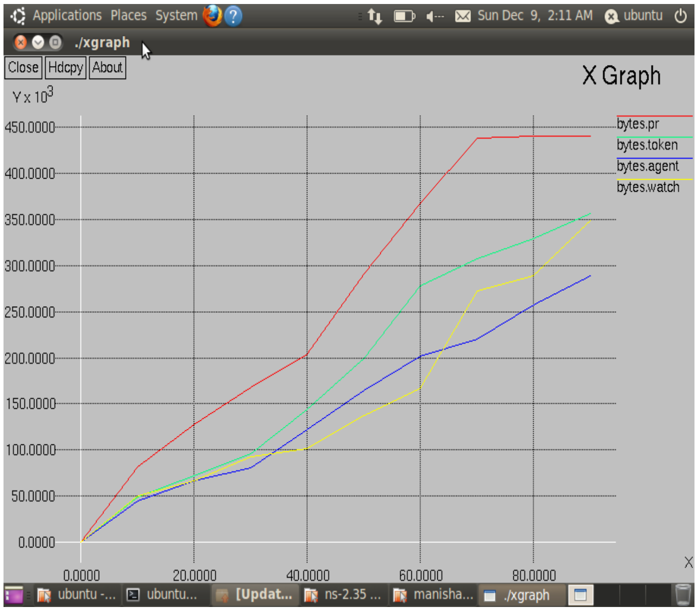

Figure 5.17 : Byte Communication based Comparative Analysis

Figure 5.17 has provided the analytical evaluation of proposed selfish node detection technique against the existing methods in terms of bytes transmission in the network. In this figure, x axis represents the simulation time and y axis represents the number of bytes transmitted in the network. Better the transmission rate, the reliable the communication method is considered. The line graph clearly shows that the bytes communication in case of proposed method is much higher than existing methods. It clearly shows that the packet transmission and communication reliability is improved in case of proposed approach.

IV CONCLUSION

The analysis is done based on the communication and cooperative behavior of nodes. The parameters computed by the agents for the mobile nodes are load, frequency, communication loss and communication delay. Once the communication and collaborative features are extracted, the fuzzy rule is applied on individual feature and identifies the criticality of each feature for each node. Later, the composite fuzzy rule is applied on these features for evaluating the degree of fuzziness for each node. Based on this fuzzy status, the isolation of normal and fuzzy attacker node is done. After the labeling of nodes, in the final stage, the AODV based routing method is applied on the safe nodes for generating the effective and reliable route over the network. The proposed agent based selfish node detection method is integrated with AODV protocol for generating the secure and reliable path.

V. REFERENCES

[1] Paul, K. and Westhoff, D., 2002. Context aware detection of selfish nodes in DSR based ad-hoc networks. In *Proceedings IEEE 56th Vehicular Technology Conference* (Vol. 4, pp. 2424-2429). IEEE.

[2] Deng, H., Li, W. and Agrawal, D.P., 2002. Routing security in wireless ad hoc networks. *IEEE Communications magazine*, *40*(10), pp.70-75.

[3] Kargl, F., Klenk, A., Schlott, S. and Weber, M., 2004, August. Advanced detection of selfish or malicious nodes in ad hoc networks. In *European Workshop on Security in Ad-hoc and Sensor Networks* (pp. 152-165). Springer, Berlin, Heidelberg.

[4] Sheltami, T., Al-Roubaiey, A., Shakshuki, E. and Mahmoud, A., 2009. Video transmission enhancement in presence of misbehaving nodes in MANETs. *Multimedia systems*, *15*(5), pp.273-282.

[5] Gupta, S., Nagpal, C.K. and Singla, C., 2011. Impact of selfish node concentration in MANETs. *International Journal of Wireless & Mobile Networks (IJWMN) Vol*, *3*, pp.29-37.

[6] Hernandez-Orallo, E., Serrat, M.D., Cano, J.C., Calafate, C.T. and Manzoni, P., 2012. Improving selfish node detection in MANETs using a collaborative watchdog. *IEEE Communications letters*, *16*(5), pp.642-645.

[7] Bawa, K. and Rana, S.B., 2015. Prevention of black hole attack in MANET using addition of genetic algorithm to bacterial foraging optimization. *Int. J. Curr. Eng. Technol*, *5*(4).

[8] Dias, J.A., Rodrigues, J.J., Xia, F. and Mavromoustakis, C.X., 2015. A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks. *IEEE Transactions on Industrial Electronics*, *62*(12), pp.7929-7937.

[9] Kumar, J.M.S.P.J., Kathirvel, A., Kirubakaran, N., Sivaraman, P. and Subramaniam, M., 2015. A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT. *EURASIP Journal on Wireless Communications and Networking*, *2015*(1), p.143.

[10] Balan, E.V., Priyan, M.K., Gokulnath, C. and Devi, G.U., 2015. Fuzzy based intrusion detection systems in MANET. *Procedia Computer Science*, *50*, pp.109-114.

[11] Lei, T., Wang, S., Li, J., You, I. and Yang, F., 2016. Detecting and preventing selfish behaviour in mobile ad hoc

network. *The Journal of Supercomputing*, *72*(8), pp.3156-3168.

[12] Hernandez-Orallo, E., Olmos, M.D.S., Cano, J.C., Calafate, C.T. and Manzoni, P., 2015. CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes. *IEEE transactions on mobile computing*, *14*(6), pp.1162-1175.

[13] Almazyad, A.S., 2018. Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks. *Neural Computing and Applications*, *29*(9), pp.597-607.

[14] Singh, R., Singh, J. and Singh, R., 2017. Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. *Wireless Communications and Mobile Computing*, *2017*.