DOI: 10.21917/ijivp.2021.0352

DETECTION OF MALEVOLENT NODES IN INTERNET OF THINGS NODES USING A TRUST BEHAVIOURAL FRAMEWORK

P.K. Swaraj[1], G. Kiruthiga[2] and K.P. Madhu[3]

[1]Department of Computer Science and Engineering, Government College of Engineering, Thirussur, India
[2]Department of Computer Science and Engineering, IES College of Engineering, India
[3]Department of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, India

Abstract

Secured internet routing in IoT has been an important study since last decade, but it has seriously threatened the data protection due to the impact of malicious nodes. An effective mechanism is therefore essential, since most of them are vulnerable to attack, to detect and prevent malicious nodes in IoT. A Trust Framework (TF) for improving diagnosis and preventing malignant nodes in IoTs is suggested in this article. This system monitors the disruptive activity of nodes in the network during agility and connectivity. It helps prevent the malicious node from affecting the packets that are run on the level of the confidence. This identification and avoidance helps to enhance packet routing with high privacy between IoT nodes.

Keywords:

IoT, Trust, Degree of Trust, Malicious Attack

1. INTRODUCTION

The Internet (IoT) is used for a large network, sensor and hop infrastructure. Network infrastructure, however, is not locked but data transfer security is conducted in a safe manner. The presence of a network safety protocol assures that all network activities are conducted normally. Various issues arising from attackers' interruption [14], poor routing and improper data transmission remain in the coordination and data exchange mechanism with other nodes. In order to prevent these issues, a confidence-based algorithm can be used between IoT nodes.

The confidence in two knots, which are attenuated by the Grey hole assault [1], Blackhole assault [1] and Jellyfish attack [7] and wormhole attack [11], [12], are described as light-weight routing protocol [1,2] with intrusion detection method. The wormhole attack was a more serious IOT threat than other threats, so in this project, safety in IoTs is improved. The confidence based protocol on source routing prevents intruders with reduced packet drop and latency [3] [5], [9] during packet transmission. The trust based QoS model measures the confidentiality level between the trust calculations direct and indirect. This raises the identification rate of malignant nodes [4]. The present study uses a new degree of trust called mutual confidence, which takes mutual trust between two nodes prominently while data is exchanged in a complete duplex model. A standard node and a node coordinator are used for self-organised key management techniques to keep security [8] by trusted certificate exchange [10]. To some degree, the research suggested is advanced with the examination of natural, malicious and multiple prevention nodes or co-ordinates for detecting the wormhole threat.

The emergence of wormhole nodes in the grid attracts more traffic in its area and an odd node behaviour is observed. Wormhole node operations are very different from standard nodes, i.e. they run at a long propagation time, have a wide communication range, and most routes are involved. The wormhole node transmission is smaller than a regular node for adjacent nodes. The wormhole node does not convey RREQ and the RREQ has to be transmitted through a private channel. Between two wormhole nodes, a tunnel is built to relay the RREQ packets. The embedded packet is lost during the node movement in the tunnel and retransmits the ordinary nodes with decreased hop counts.

The suggested Trust Framework (TF) framework is used to prevent such impacts on IOTs. It incorporates a confidence-driven identification model and an avoidance model based on nodes. The system was developed with the aim of sending the RREQ packet to fewer wormhole nodes than standard nodes. By absolute, indirect or shared confidence, the proposed approach therefore estimates the trust in two nodes at first. If a trust between two nodes is established, the prevention node helps spread the authenticity of the two nodes across the network to all nodes. If no shared confidence exists between two nodes, the node is called malicious, and all nodes of the network receive a threat or block alert. This node is isolated from ordinary nodes.

2. TRUST DETECTION MODEL

The trust relationship between network nodes is discussed in this section. The value of the trust between the nodes is taken into account in absolute and indirect confidence.

2.1 DIRECT TRUST

The direct trust model is calculated to a certain degree in terms of node communication, active node cooperation and network association that defines the extent of the trust. In terms of its subjective behavior, which is an obvious example of the direct confidence degree, this direct confidence provides a relation between nodes. This is a detailed study of the degree of direct confidence using similarity and node tie power. Similarly, the analysis of distance between the nodes of the indirect trust degree is carried out.

There is still homogeneity of network nodes, i.e. identical nodes are correlated. By comparing the cumulative mutual neighbors between two nearby sensor knots, the similarity of the node is measured. When there is a higher similarity between nodes, the neighboring nodes often overlap. The current node therefore gives a considerably lower similarity to a larger number of neighboring nodes.

2.2 INDIRECT TRUST

Indirect trust takes the transfer of information between nodes into account. Due to non-adjacent nodes there are indirect connections that can be opened through intermediate nodes. This results in an indirect reliance on the non-adjacent nodes that is estimated via the direct confidence model among the neighboring nodes. Single and multi-path methods take varying shapes of the transmission confidence between the source and destination node.

2.3 MUTUAL TRUST

Between nodes using a direct trust model and indirect trust model, the trust value is estimated. The trust between the pairs of nodes is always not the same and it is justified as the directional node. Furthermore, a node that has sent a message cannot be reported to the presence of malicious nodes. This induces an extraordinary behaviour in neighboring sensor nodes, i.e. confidence disparities. This affects the precision of confidence-based identification. The non-directional model is therefore required to build mutual confidence between nodes. Turning node confidence into shared confidence addresses odd node activity and decreases the limitation of trust level detection with increasing accurate measurements.

3. PREVENTION FRAMEWORK

The proposed confidence detection system, based on its function, has normal, malicious and prevention nodes.

- Normal nodes are commonly found in a network sending data transfers. The regular node lists or joins the malicious nodes in the prevention node block table. It drops malicious nodes from data packets, Hello, RREP, and RREQ.
- Malicious Nodes collects and transmits RREQ message to a whole network. Hop counts are not increased by the broadcast of malicious nodes. The RREP message will be sent again along the same direction, where other additional paths are involved. Now the source nodes believe that the routes through these nodes are short and therefore communication is established by these routes.
- Prevention Nodes detects and blocks suspicious nodes. These nodes have a status field overview table defining the prevention node set. The Suspected Value field represents an approximate suspected value for nodes. The Suspicious Node confirmation field indicates the alert or block message that has been broadcast against malicious nodes. Finally, the message block and threat is provided in the message table of block and threat.

The overall number of preventative nodes depends completely on the range and area of the network. This research is performed through a whole network deployment of the prevention node and direct communications with other nodes. Total prevention nodes are estimated by,

$$\text{Prevention Node} = \left(\frac{X}{r}-1\right)\left(\frac{Y}{r}-1\right) \tag{1}$$

where,

X - network length,

Y - network width and

r - transmission range by prevention node.

This algorithm to achieve better results in identification using behavioral definition, the confidence grade estimate between two nodes is carried out and stored statistically in the local file system.

4. EXPERIMENT RESULTS AND ANALYSIS

Control is taken on the E6700 3.2 GHz 4GB RAM for the confidence measurement and wormhole identification. The confidence estimate is programmed using R using the iGraph toolkit, and the identification of wormholes is performed with NS 2.34. The Table.1 shows the parametric values necessary to carry out the experiments.

Table.1. Simulation parameters

Parameters	Value
Area	$1500\times1500\text{m}^2$
Transmission range	250 m
Protocol	AODV
Time	500 s
Mobility	Random mobility
Size of data packet	512 bytes
Type of Traffic	CBR
Maximum speed of packets	25 ms^{-1}

In a fixed spot, 18 prevention nodes and 50 regular nodes are experimented with the output of the proposed device using the AODV protocol. The RREQ packet is retrieved from another malicious node and retransmitted at frequent intervals by updating the route. The Packet RREQ has fewer hop numbers than the other nodes and supports other routes in wormhole nodes. It also removes the other nodes from the originating node to drop data packets.

The wormhole nodes in the network that are fixed in a given position can be easily detected. Since even regular nodes are easier to track the activity of malicious nodes, before they are transmitted as malicious nodes. On the other hand, when nodes are on the mobile, it is hard to find malicious nodes on the network. While the malicious nodes are removed from the control node range and join the range of other monitoring nodes. The first node monitoring data is thus assumed to be inutile. The approach suggested using the preventive node to exchange malicious node information with other nodes by means of a message of danger to avoid such consequences.

4.1 PACKET DROP RATE

The packet drop rate for a pause from 0 to 20 Honeypot with eight fixed worm holes and mobile wormhole nodes can be seen in Table.2. For the proposed model, the average packet drop rate for fixed wormhole and mobile wormhole nodes is 25.9% and 28.4%, respectively.

Table.2. Packet drop rate

Trust Models	Nodes				
	100	200	300	400	500
Direct Trust	10.5	11.8	15.5	11	13.5

Indirect Trust	9.6	11.6	15.2	10.9	13.4
Mutual Trust	16.5	17	19.6	17	16
D+ID+MT	20.5	19	19.6	17	16

4.2 FALSE POSITIVE RATE

The Table.3 shows the false positive rate difference between the direct, indirect and mutual trust models. The average fake positive rate of direct and indirect is 9.7% and 12.5%, respectively. Similarly, for fixed wormhole and mobile wormhole nodes, the average false-positive rate is 0.4% and 0.1%, respectively.

Table.3. False Positive Rate

Trust Models	**Nodes**				
	100	**200**	**300**	**400**	**500**
Direct Trust	0.2	0.5	0.6	0.7	1
Indirect Trust	0.2	0.3	0.4	0.6	0.7
Mutual Trust	8.5	10.6	9.6	12.5	6
D+ID+MT	17	11	9.8	12.5	7.5

4.3 WORMHOLE DETECTION TIME

The detection time differential for eight fixed and mobile nodes as seen in Table.4. The mean Honeypot detection times for fixed wormhole and mobile wormhole nodes are 300s and 354s, respectively. Similarly, the average detection time for fixed wormhole and mobile wormhole nodes in TF is 149 and 169s, respectively.

Table.4. Wormhole detection time

Trust Models	**Nodes**				
	100	**200**	**300**	**400**	**500**
Direct Trust	140	139	145	195	165
Indirect Trust	155	175	190	210	165
Mutual Trust	310	360	275	280	255
D+ID+MT	390	415	380	290	320

5. CONCLUSIONS

This paper presents an Internet paradigm for trust-based detection and avoidance of wormhole attacks. The aim of this approach is to check each node confidence level and prevent the wormhole network from upsetting the packet flow. The model of prevention reduces the number of RREQ packets to the neighboring nodes. Since regular nodes detect the wormhole node correctly, we then use the network avoidance node to locate the malicious nodes. This node helps locate and remove the RREQ post, but not in regular routing. The outcome demonstrates a higher identification of wormhole nodes by the proposed TF. The TF approach proposed avoids wormhole activity affecting the standard node, reducing detection time compared to Honeypot. It prevents the dissemination and prolonged existence of false information in the network by considering the identification node.

REFERENCES

[1] T. Karthikeyan and K. Praghash, “An Improved Task Allocation Scheme in Serverless Computing using Gray Wolf Optimization (GWO) based Reinforcement Learning (RIL) Approach”, *Wireless Personal Communications*, Vol. 117, No. 3, pp. 1-19, 2020.

[2] S. Kannan, G. Dhiman, and M. Gheisari, “Ubiquitous Vehicular Ad-Hoc Network Computing using Deep Neural Network with IoT-Based Bat Agents for Traffic Management”, *Electronics*, Vol. 10, no. 7, pp. 785-796, 2021.

[3] N.V. Kousik, “Analyses on Artificial Intelligence Framework to Detect Crime Pattern”, Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, pp. 119-132, 2021.

[4] A.S. Nandhini and P. Vivekanandan, “A Survey on Energy Efficient Routing Protocols for MANET”, *International Journal of Advances in Engineering and Technology*, Vol. 6, No. 1, pp. 370-381, 2013.

[5] N.G. Veerappan Kousik, K. Suresh, R. Patan and A.H. Gandomi, “Improving Power and Resource Management in Heterogeneous Downlink OFDMA Networks”, *Information*, Vol. 11, No. 4, pp. 203-216, 2020.

[6] K.W. Kim, Y.H. Han and S.G. Min, “An Authentication and Key Management Mechanism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks”, *Sensors*, Vol. 17, No. 10, pp. 1-20, 2017.

[7] G. Dhiman, K. Somasundaram and K. Sharma, “Nature-Inspired-Based Approach for Automated Cyberbullying Classification on Multimedia Social Networking”, *Mathematical Problems in Engineering*, Vol. 2021, pp. 1-21, 2021.

[8] P.K. Dhillon and S. Kalra, “Multi-Factor User Authentication Scheme for IoT-Based Healthcare Services”, *Journal of Reliable Intelligent Environments*, Vol. 4, No. 3, pp. 141-160, 2018.

[9] A.K. Das, P. Sharma, S. Chatterjee and J.K. Sing, “A Dynamic Password-Based User Authentication Scheme for Hierarchical Wireless Sensor Networks”, *Journal of Network and Computer Applications*, Vol. 35, No. 5, pp. 1646-1656, 2012.

[10] N.V. Kousik, P. Johri and M.J. Divan, “Analysis on the Prediction of Central Line-Associated Bloodstream Infections (CLABSI) using Deep Neural Network Classification”, *Proceedings of International Conference on Computational Intelligence and Its Applications in Healthcare*, pp. 229-244, 2020.

[11] P. Johri, “Improved Energy Efficient Wireless Sensor Networks using Multicast Particle Swarm Optimization”, *Proceedings of International Conference on Innovative Advancement in Engineering and Technology*, pp. 1-6, 2020.

[12] S. Kannan and S.N. Mohanty, “Survey of Various Statistical Numerical and Machine Learning Ontological Models on Infectious Disease Ontology”, *Proceedings of International Conference on Data Analytics in Bioinformatics: A Machine Learning Perspective*, pp. 431-442, 2021.

[13] D.S.K. Tiruvakadu and V. Pallapa, “Confirmation of Wormhole Attack in MANETs using Honeypot”, *Computers and Security*, Vol. 76, No. 2, pp. 32-49, 2018.

[14] S. Jayasri, A. Daniel and P. Rajakumar, “A Survey on Various Load Balancing Algorithm to Improve the Task Scheduling in Cloud Computing Environment”, *Journal of Advance Research in Dynamic Control Systems*, Vol. 11, No. 8, pp. 2397-2406, 2019.

[15] M.N. Ahmed, A.H. Abdullah, H. Chizari and O. Kaiwartya, “F3TM: Flooding Factor based Trust Management Framework for Secure Data Transmission in MANETs”, *Journal of King Saud University-Computer and Information Sciences*, Vol. 29, No. 3, pp. 269-280, 2017.