A CORRELATED BAYESIAN GAME THEORY WITH EXTENDED CREDIT SCORE FOR IDENTIFYING MALICIOUS AND SELFISH NODE IN MANET

S. Sampath and S. Veni
Department of Computer Science, Karpagam University, Coimbatore, Tamil Nadu, India
E-Mail: sampathphd2016@gmail.com

ABSTRACT

Mobile ad hoc network (MANET) is infrastructures less, dynamic, localized network of wireless mobile nodes. MANET nodes are relies upon network cooperation mechanism to correctly work, forwarding traffic unrelated to its personal use. In early work Bayesian Correlated Equilibrium based IDS for MANET is used for detecting the malicious node and normal node in the network. In this network some nodes selfishly decide to employ partially. The presence of selfish node within the MANET may reduce performance degradation of Network. So, the MANET requires detecting the Selfish node and improves the cooperation of each node. In this paper proposed the extended credit score (xCR) with game theory to detect selfish nodes as well as malicious nodes. An efficient proposed method constructs with maximum accuracy and less computational overhead to detect malicious and selfish node detection along with Bayesian correlated Equilibrium based intrusion detection system.

Keywords: MANET, correlated equilibrium, game theory, extended credit score, intrusion detection system.

INTRODUCTION

MANET (Hernandez-Orallo, E., *et al.* 2012) is the wireless adhoc network. The MANET is a network with many independent nodes such as mobile devices. The MANET is utilized dynamic topology, wireless links, decentralized network and does not want any cellular infrastructure. The each node in MANET moves independent of its place due to that the topology of the group modifications dynamically. So the user need to provide safety to the data packets transmitted among the nodes through the reputable routes. It is a plane network, the main functions of MANET is node mobility and dynamic topology. Those two principal capabilities are the purpose for the attacks. Malicious user may additionally attempt to attack the facts packets by way of tracing the path. The malicious attackers may attempt to explore the source and destination through different kind of attacks. The applications of MANET are in army warfare field, sensor networks, commercial sectors, clinical sectors.

In early work the Bayesian Correlated Equilibrium based IDS for MANET (Subba, B., *et al.* 2016) used and this strategy is efficiently used to reduce the IDS traffic and power consumption of nodes. Since it has some vulnerability like lack of centralized authority, limited bandwidth, limited power supply, limited availability of resource, dynamic topology, and routing overhead etc.., MANET is assumption that each node is co-operative and trusted. However in the fact, a number of nodes may additionally act selfishly and (Subramaniyan, S., *et al.* 2014) they do not longer cooperate with neighbour nodes in the network. If the every node of the network makes a decision to act selfishly the complete network can be collapsed.

In this paper the Extended Credit Score (xCR) with game theory has been proposed to identify selfish nodes as well as attack node. In this approach the three main basic components are used to find out the selfish or attack node, such as the player, strategy and utility or payoff. The each player is referred to the number of participant; the strategy is termed as the rules of selection of action by the players. Then finally the utility unction used to refer whether selfish node or malicious node based on the payoff value.

RELATED WORK

Improving Selfish node detection in MANET (Hernandez-Orallo, E., *et al.* 2012) proposed collaborative watchdogs to detecting selfish nodes. If the one selfish node was predicted early in the MANET Network it's distribute the information about to other nodes. After that in the node was positive then it's known as the selfish node. The result shows that the present approach was minimized the detection time and cost.

Effect of selfish node in MANET (Gupta, S., *et al.* 2011) presented to analyse the causes of selfish node in the network. The presence of selfish node in the network was reduced the loss of power with time. If the time passes away the nodes lose their battery energy then its possible recharge in disaster area. However the present technique has less throughput and high overhead.

Selfish node Detection in MANET (Koshti, D., & Kamoji, S. 2011) presented new approach to detect selfish node in MANET. The new approach was performed based on Reputation and credit techniques. The credit technique was offered the incentives for nodes to automatically employ the networking functions. Initially the virtual currency or similar payment system build the setup and then the nodes get pain for deliver the services to other nodes. Then additionally an auction based AODV protocol approach was introduced to the auctions for adhoc network which contains the selfish nodes. Since the present technique increase the energy consumption in nodes.

Selfish Node Detection in MANET's (Hernández-Orallo, E., *et al*. 2012) proposed the collaborative watchdog methods to detection of selfish node for reduce the effect of false positives and false negatives. The Analytical model was presented to evaluate the detection time and induced the overhead of the collaborative watchdog. However the present technique does not provide the correct solution for energy consumption.

Malicious Node Detection System for MANET (Rajaram, A., & Palaniswami, S. 2010) proposed MAC layer security protocol to reach confidentiality and authentication of data packets in MANETs. Initially the trust based packet forwarding scheme was detected the malicious nodes. Then second phase of the protocol the link layer security utilized to CBC-X mode of authentication and encryption. However the MAC layer takes long time to find all the path and shares the time slots between the neigh boring nodes.

Performance Comparison of Single and Multipath Routing Protocol (Sangi, A. R., *et al*. 2010) based of selfish behaviors. Based on the existing selfish behavior the new variation analysed. The multipath protocol performs more efficient than single path to reduce the selfish node. The multipath link disjoint direction with selfish nature become more efficient and offered more number of paths than its counterpart of the disjoint path choice among any order pair of nodes. So the single path routing protocol require secure feedback mechanism to generate the routing protocol.

Selfish Node detection related to Mobile Agent (Roy, D. B., & Chaki, R. 2011) proposed new intrusion detection system (IDS) under Mobile Agents. The set of mobile agents used to reduce the network bandwidth consumption. The result shows that the proposed technique reduces the computation overhead for each node in the network.

Selfish Node Detection in MANET (Das, D., et.al.2015) presented the game theoretic approach to lowering the selfish node. On this mechanism suppose the direction damaged due to selfish node then mechanically chosen the available direction for next facts transmission in the network. The result suggests that the existing approach assures low cost data information transfer and smallest amount of idle time.

Classification of Nodes in MANET (Akhtar, A. K., & Sahoo, G. 2013) proposed mathematical classifier model in MANET's. The proposed model was categorized into selfish node and normal node as well as allocated the grade to the individual nodes. The grade was assigned depends on the number of passes the algorithm to classify the node and also describe the punishment strategy as well as the improvements of the description of the reputation conventional based mechanisms. The present technique applicable for only limited resources.

Selfish Node Attack in MANET (Soni, G., & Chandravanshi, K. 2013) proposed intrusion detection algorithm is to find the selfish node and removed the misbehavior activities. The malicious node was the major critical factor for reducing the performance of the routing protocol, the acknowledgement of the TCP demonstrates due to fake information in network the most of the senders are not obtain the acknowledgement from receiver means all the acknowledge are lost. After applying the Intrusion detection system scheme on every node which is take part in routing will show the information of ACK packets. Since the present technique security protocols for the wired networks cannot work for ad hoc networks.

Collaborative selfish node detection (Ciobanu, R. I., et al. 2014) proposed the SENSE, selfish node detection in the network. Since the local information is not sufficient to reach the informed decision, the nodes running SENSE collaborate via gossiping, to the detection of selfish node. The result shows that it behaves better in terms of network performance and detection accuracy. Since the present technique does not perform well in uncertain situation.

Gradual solution to detect selfish nodes (Djenouri, D., & Badache, N. 2010) present the new monitoring solution which was used to mitigates the limitations of the watchdog based monitoring, named the two hop acknowledgement via the use of the lower layer acknowledgement was reduced gradually. The present technique was also applicable even though the power control mechanism used. However the volatile network topology makes it hard to detect malicious nodes.

Research Methodology

This paper proposes Bayesian Correlated equilibrium based selfish node detection for MANET with objective such as detection of selfishness of each node and malicious node by using Extended Credit Score (xCR) with correlated equilibrium, reduce the computation overhead of each node and improve the detection of selfish node with high detection rate and accuracy.

Extended Credit Score (xCR)

The detection of selfish node and malicious node is related on the idea of credit risk (CR) score. The each and every node is computed the CR score within the network. Based on these CR score the each node is estimated the level of selfishness or malicious node for all connected nodes,

Before proceeding the CR score first require to compute the abnormal node alarm of N_k onN_i, represented as P_i^k

$$P_i^k = \frac{\text{the number of } N_i \text{ data requests not served by the expected node } N_k}{\text{the total number of } N_i \text{ is requests for data allocated to } N_k} \quad (1)$$

The equation (1) can be approximated by N_i during query processing time, thus P_i^k is represented the ratio ofN_i's data requests not served by the expected nodeN_k. The estimated abnormal node alarm, the CR score is computed by equation (2)

$$CR_i^k = \frac{P_i^k}{\alpha * SS_i^k + (1-\alpha) * ND_i^k}, \text{ Where } 0 \leq \alpha \leq 1 \qquad (2)$$

SS_i^k, ND_i^k- represented the size ofN_k's shared memory space and the number ofN_k's shared data items for N_i.

The both SS_i^k, ND_i^k areN_i's estimated values since the N_k may be selfish or attack and its does not need the N_i is the countable number of shared data items and countable number of shared memory space. Then the system parameter α is used to adjust the importance of theSS_i^k and ND_i^k. The value of P_i^k (as well asSS_i^k and ND_i^k) is updated each and every processing time. Then the node updates at CR_i^k at every processing time and look up for the connected nodeN_k at every relocation time. Furthermore the each node has its own threshold δ ofCR_i^k. The measure of CR_i^k is exceeded δ the node N_k detects the selfish node or malicious node by the N_i.

The effect of parameters SS_i^k, ND_i^k on CR_i^k are weighted by considering the allocated space at node N_i, represent as S_i and the total number of data items accessed by the N_i which is represent as n_i. The rationale is that the CR_i^k may be strongly affected by the S_i and n_i, if CR_i^k is not normalized, its normalized by Equation (3) where the nCR_i^k stands for the normalized CR_i^k

$$nCR_i^k = \frac{P_i^k}{\alpha * \frac{SS_i^k}{S_i} + (1-\alpha) * \frac{ND_i^k}{n_i}} \text{ , Where } 0 \leq \alpha \leq 1 \qquad (3)$$

In the Bayesian network the each node utilized the extended Credit Risk (xCR) score to estimate the integrated degree of selfishness or malicious node level for all connected nodes including selfish nodes and malicious nodes. However the faraway nodes are intend to be frequently disconnected and produce the false alarms, and then include the distance in terms of number of hops, which is represent as H, in to the level of selfishness or malicious node. The following equation (1) used to measure the integrated degree of selfishness or malicious node level.

$$xCR_i^k = nCR_i^k * \left(\frac{H_i^k}{\max H_i}\right)^2 \text{Where } 0 \leq \alpha \leq 1 \qquad (4)$$

H_i^k - Denoted the number of hops between N_i and N_k

$\max H_i$ - Denoted the maximum H_i^j for connected node N_j

N_i - Get the number of hops as H_i^k between two nodes and $\max H_i$ using the information from Bayesian network.

Bayesian game model for detecting selfish node and malicious node based on extended score value

In the Bayesian network the normal node which is free from selfish behavior and any other malicious node are detected by using the payoff matrix or if the limited threshold value is exceed the malicious node or selfish node removed from the network.

The proposed system has mainly consists of three basic components such as set of players (P), a set of actions (S) and utility function (U).

Players: The players are the decision makers in the game model. There are two or more decision makers in each game known as the players.

Strategy: the strategy is used to refer the rules of selection of action by the players.

Utility: the each player has the range of possible outputs and clear the order of performance depends on payment. The aim of the game is to be and maximize the utility function of each player. Find out the normal to which is free from attack and selfish behavior.

A game is defined as the G= (P; S; U)

P - Countable Number of players or nodes of the network

S - Strategy set of the node
Assume the S_i is the strategy space of the node i or the number of strategies available for node i.

U - Utility function of a node or payoff of a node. The U_i denote as the utility function or payoff of node i.

In the game theory, one nodes send packets to other node and then decide whether the normal node, selfish node and malicious node their respective Extended credit score value.

Malicious node detection based on extended score value

In the two player game,

Players: Three nodes namely Potential attacker and potential defender

Strategy: For the potential attacker Malicious node or Normal Node.

For the defender player {Monitor, Not Monitor}

The strategies are chosen by the players in the initial stage of the game based on the Extended Score value in monitoring and malicious any given node in the network.

Let G= {P, S, U} where N= $\{P_i, P_j\}$ the players of the game, then the S=$S_i X S_j$ the strategy space of the players, U=$U_i X U_j$ is the pay off utility corresponding to the strategy space S of the game. The U_i and U_j for the players respectively. The C is the cluster nodes with C= $\{n_1, n_2, n_3 \dots\dots\dots n_{xCR}\}$. Then consider the any node n_{xCR} in the cluster, with the asset value w_{xCR}.

The payoff values corresponding to the interaction between the attacker and defender is calculated on the basis of the reputation value of the node n_k, the extended credit score involved in the attack C_{axCR}, monitoring cost C_{mxCR}, detection rate, false alarm rate (α) etc. Table-1 explain the payoff values when the type of attacker player is malicious node.

Selfish node detection based on extended score value

In the two player game

Players: Three nodes namely Normal Node, Partially Selfish Node and Selfish Node.

Strategy: Either Normal node, partially selfish node or selfish node.

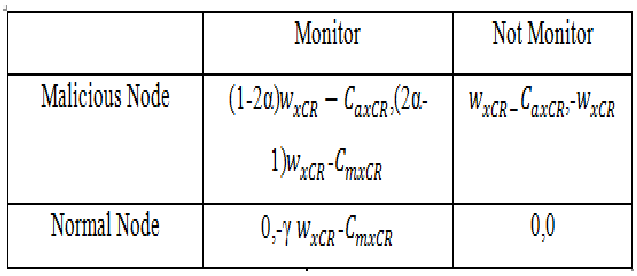
Utility or Payoff: when the one node is forward to the other packets of node it get the pay off else if its act as the selfish node or attack node does not forward other packets of the nodes it will does not get the any pay off.

Assume the three nodes namely Normal node, partially selfish node and Selfish node. The every node is intermediate node of path from the source node to destination node. Consider the extended credit factors of three nodes are XxCR. If the node is normal nodes it's send the packets to other nodes and get the benefits. Else in the node is partial selfish node it may send the packets to other nodes mean get the benefits. Else the node is selfish node means does not send any other packets and it will not get any benefits.

From the Table-2 it's clear the payoff off node is always X_{xCR}, however it always forward the packets of all other node. But the partial selfish node or selfish node will receive X_{xCR} payoff when it forward the packet of other node and it will not receive any payoff if it does not forward. So, clearly know that the forwarding other node's packet is always benefits for normal node.

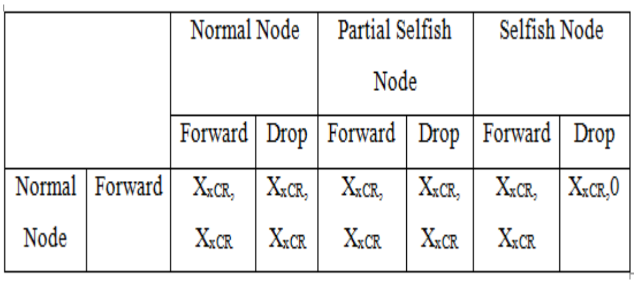
So the utility function of the intermediate node $U=X_{xCR}$ is better when the node forwards packet to other node. This is promoting to the cooperation in the network. The Table-2 represents the payoff matrix for Normal node, Partially Selfish node and Selfish Node. The Table-3 represents the when the node is normal.

Table-1. Payoff matrix for malicious node.



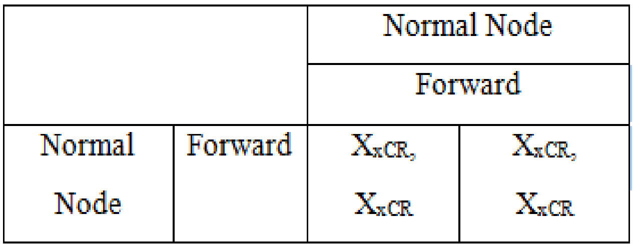
	Monitor	Not Monitor
Malicious Node	$(1-2\alpha)w_{xCR} - C_{axCR},(2\alpha-1)w_{xCR}-C_{mxCR}$	$w_{xCR}-C_{axCR},-w_{xCR}$
Normal Node	$0,-\gamma\, w_{xCR}-C_{mxCR}$	0,0

Table-2. Payoff matrix for normal node, partial selfish node and selfish node.



		Normal Node		Partial Selfish Node		Selfish Node	
		Forward	Drop	Forward	Drop	Forward	Drop
Normal Node	Forward	X_{xCR}, X_{xCR}	X_{xCR}, X_{xCR}	X_{xCR}, X_{xCR}	X_{xCR}, X_{xCR}	X_{xCR}, X_{xCR}	X_{xCR},0

Table-3. Payoff matrix for two normal nodes.



		Normal Node	
		Forward	
Normal Node	Forward	X_{xCR}, X_{xCR}	X_{xCR}, X_{xCR}

Bayesian correlated equilibrium

The game between the normal node, selfish node and malicious node in case the normal node does not aware of whether the node is normal or malicious. Thus it assumed the three nodes has the goal to maximize their pay off value. So that the normal node increase the probability of getting the payoffs based on the Extended Credit Score value and the selfish node and malicious node does not getting any payoff.

A correlated equilibrium determines an effective solution when there is an extensive game in the network between the players. Thus this equilibrium is a correlated strategy for the players implemented by a mediator that makes non binding recommendations to each player. Assume that there is a mediator that recommends a particular strategy to players. Based on the recommendation, the player can choose it or option other strategy from its set.

Correlated equilibrium

a) Assume the number of player learnt simple strategy to that participant by means of the mediator.

b) Suppose the mediator advice the normal node for player 1, and then the player knows that the normal node is recommended for packet forwarding of other nodes. Thus the normal node forward to the packets it is the best response for other nodes. So the player 1 would be happy to forward by accepting the recommendation of the mediator.

c) Assume the mediator recommends selfish node for the participant i, knowing that the mediator would have possibly have advice does no longer forwarding some other packets within the network. When the selfish node or attack node does not forward of any other packets of other nodes the normal node gets the benefits.

d) Thus the selfish node and malicious node does not consider the mediator recommendation.

From the sequence, it does understand that the selfish node and malicious nodes are listened to the mediator. Generally the normal node chooses the mediator's opinion under the belief that selfish node and malicious node obey the mediator. This indicates that the gamers can attain the self imposing understanding to obey the mediator if the mediator recommends the correlated method.

Let K belongs to the Δ(S) be the correlated strategy recommended by the mediator. And K is the knowledge. The Strategy K induce an equilibrium for the two players to obey the mediator if

$$\sum_{s\in S} K(S_i,S_j)U\,(S_i,S_j) = U(K) \geq \sum_{s\in S} K(S_i,S_j)U\,(\delta(S_i),S_j) \tag{5}$$

Where $\delta(S_i)$ is the strategy that player i obeys the mediator. Such a strategy K is called a correlated equilibrium.

$$\sum_{s\in S} K(S_i,S_j)[U\,(S_i,S_j) - U\,(S_i{}',S_j) \geq 0 \tag{6}$$

Equation (6) shows the strategy when player I disobeys mediator, and also to expect a payoff. it is to be noted that K(S)≥ 0 for all values of S. Such that

$$\sum_{s\in S} K(S) = 1 \tag{7}$$

It can be shown that the set of all correlated equilibrium in a finite game is a compact and convex set.

The feasible solution is obtained by solving the linear problem,

$$\max \sum_{i,j} U_{i,j}(K) \tag{8}$$

That subjects to $\sum_{s\in S} K(S_i,S_j)[U\,(S_i,S_j) - U\,(S_i{}',S_j) \geq 0$ and

$$\sum_{s\in S} K(S) = 1.$$

An optimal solution of this linear program will give a correlated equilibrium that maximizes the selfish node and malicious node detection in the Bayesian network.

Thus this equilibrium state determines the probability value to activate the heavy weight module to analyze the selfish node and malicious node then reduce its abnormal threshold value and remains the same if it is normal.

RESULT AND DISCUSS

The proposed Extended Credit Score (xCR) with game theory for MANET is tested for its effectiveness using the performance parameter such as Packet Delivery Ratio, Detection Rate, Throughput and Delay. These parameters are evaluated and compared with the existing Bayesian Correlated Equilibrium based IDS technique to prove that the proposed scheme outstands from all other existing IDS techniques.

Packet Delivery Ratio (PDER)

The Packet Delivery is used to calculate how much number of packets forwarded to the destination node against number of packets generated by the same node.

$$\text{PDER}=\frac{\textit{Number of packets Transmitted by node}}{\textit{Total number of incoming packets}}$$

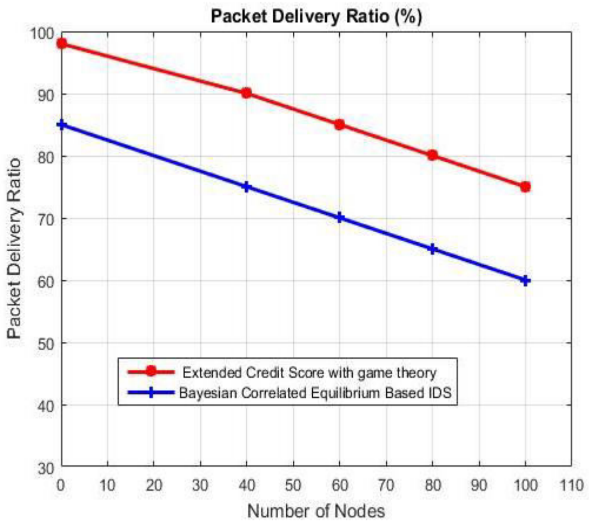


Figure-4.1. Packet delivery ratio comparison.

Figure-4.1 shows the Packet delivery Ratio (PDER) Comparison of the Bayesian Correlated Equilibrium based IDS technique and the proposed Extended Credit Score (xCR) with game theory for MANET. The PDR value of the two schemes is evaluated for increasing number of nodes in the network. The comparison result show that the proposed method stands out in high packet delivery ratio.

Detection rate

The Detection rate is used to refer the number if intrusion instances detected by the system (True Positive) divided by the total number o intrusion instances place in the test set.

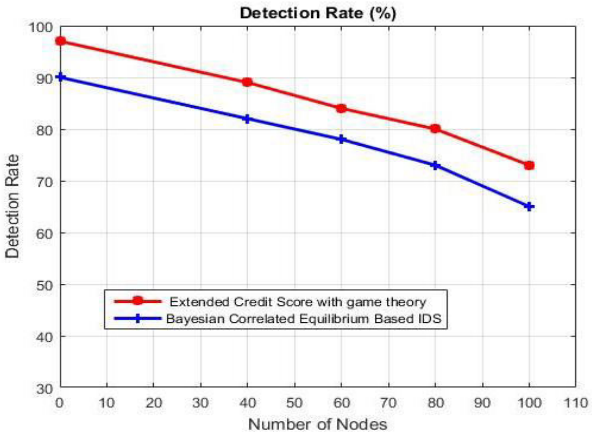


Figure-4.2. Detection rate comparison.

Figure-4.2 shows the Detection Rate Comparison of the Bayesian Correlated Equilibrium based IDS technique and the proposed Extended Credit Score (xCR) with game theory for MANET. The Detection Rate value of the two schemes is evaluated for increasing quantity of malicious node in the network. The comparison result shows that the proposed approach has the advanced detection rate than Bayesian Correlated Equilibrium based IDS.

Network throughput

The Network throughput is referred the rate of successful message delivery in the communication channel.

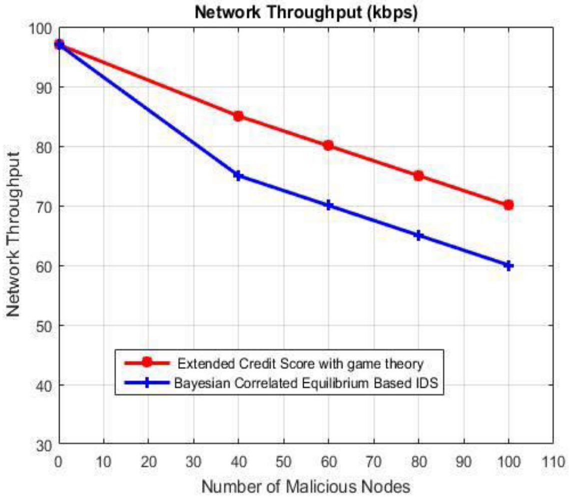


Figure-4.3. Network throughput comparison.

Figure-4.3 shows the Network Throughput Comparison of the Bayesian Correlated Equilibrium based IDS technique and the proposed Extended Credit Score (xCR) with game theory for MANET. The Network throughput value of the two schemes is evaluated for increasing quantity of malicious node in the network. The comparison result shows that the proposed approach has the high network throughput than Bayesian Correlated Equilibrium based IDS.

Detection delay

The detection delay is referred the time delay in detecting the mobile intruders in the network by the defender or the IDS itself.

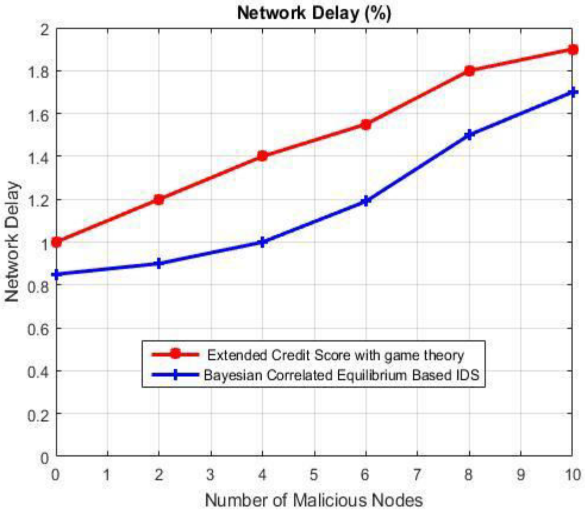


Figure-4.4. Network delay value comparisons.

Figure-4.4 shows the Network Delay Value Comparison of the Bayesian Correlated Equilibrium based IDS technique and the proposed Extended Credit Score (xCR) with game theory for MANET. The Network delay of the two schemes is evaluated for increasing quantity of node in the Network. The result shows that the proposed approach achieves quicker to detecting the malicious nodes inside the Network.

CONCLUSIONS

The proposed Extended Credit Score (xCR) with game theory is effectively identify selfish nodes as well as malicious nodes. In this approach mainly consists of three basic components such as players, strategy and utility. The players used to identify the number of participant in the network. The strategy is related on the node forward or drop packet to other nodes. Then finally the utility or pay off function used to identify whether it is normal, selfish or malicious nodes based on the extended credit score (xCR) value. If the nodes is does not get any pay off that node has the selfish node or malicious nodes. The proposed approach performs better than the Bayesian Correlated Equilibrium based IDS for MANET in terms of Packet Delivery Ratio, Detection Rate, Network throughput and Detection Delay.

REFERENCES

[1] Hernandez-Orallo E., Serrat M. D., Cano J. C., Calafate C. T. & Manzoni P. 2012. Improving selfish

node detection in MANETs using a collaborative watchdog. IEEE Communications letters. 16(5): 642-645.

[2] Subba B., Biswas S. & Karmakar S. 2016. Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. Engineering Science and Technology, an International Journal. 19(2): 782-799.

[3] Subramaniyan S., Johnson W., & Subramaniyan K. 2014. A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. EURASIP Journal on Wireless Communications and Networking. 2014(1): 205.

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

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

[6] Koshti D. & Kamoji S. 2011. Comparative study of techniques used for detection of selfish nodes in mobile ad hoc networks. Int J Soft Comput Eng (IJSCE). 1(4): 190-194.

[7] Hernández-Orallo E., Serrat Olmos M. D., Cano J. C., Calafate C. T. & Manzoni P. 2012. Evaluation of collaborative selfish node detection in MANETS and DTNs. In Proceedings of the 15th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems (pp. 159-166). ACM.

[8] Rajaram A. & Palaniswami S. 2010. Malicious node detection system for mobile ad hoc networks. International Journal of Computer Science and Information Technologies. 1(2): 77-85.

[9] Sangi A. R., Liu J. & Liu Z. 2010. Performance comparison of single and multi-path routing protocol in MANET with selfish behaviors. World Academy of Science, Engineering and Technology. 41, 828-832.

[10] Roy D. B. & Chaki R. 2011. MADSN: Mobile agent based detection of selfish node in MANET. International Journal of Wireless & Mobile Networks (IJWMN). Vol. 3.

[11] Das D., Majumder K. & Dasgupta A. 2015. Selfish node detection and low cost data transmission in MANET using game theory. Procedia Computer Science. 54, 92-101.

[12] Akhtar A. K. & Sahoo G. 2013. Classification of selfish and regular nodes based on reputation values in MANET using adaptive decision boundary. Communications and Network. 5(03): 185.

[13] Soni G. & Chandravanshi K. 2013. A Nobel Defence Scheme against Selfish Node Attack in MANET. arXiv preprint arXiv:1307.3638.

[14] Ciobanu R. I., Dobre C., Dascălu M., Trăuşan-Matu Ş. & Cristea V. 2014. Sense: A collaborative selfish node detection and incentive mechanism for opportunistic networks. Journal of Network and Computer Applications. 41, 240-249.

[15] Djenouri D. & Badache N. 2010. A gradual solution to detect selfish nodes in mobile ad hoc networks. International Journal of Wireless and Mobile Computing. 4(4): 264-274.