An Energy-Efficient Intrusion Detection System for MANET

Preeti Pandey and Atul Barve

1 Introduction

Mobile ad hoc network (MANET) [1] refers to a decentralized network. It has a number of stations that are free without any supervision of authority. This network structure depends on the number of movable nodes and thus it is infrastructure less. This structure does not have any access points or cables, routers and servers. In MANET, nodes are capable to move without restraint. So, these may alter their locations as required. A node can act as a source or as a destination at a time and one of them may possibly become a router. It performs every task and forwards packets to the next nodes. Mobile ad hoc networks have several features such as restricted bandwidth; inadequate power supply for all nodes and dynamic topology of network, etc., the important reason is the steady change in the network configuration because of high degree of mobility of nodes. Mobile network plays a vital role for communication among the troops in military operation. Some of the applications of MANET are medical surveillance, traffic control, disaster management, etc.

MANET is used in various places and has much importance. In MANET, for routing when AODV is used [2] or minimum intermediate hop count, if DSR is applied [3] the sender sends actual data through particular link after receiving the path but simultaneously many senders use the same link. Thus, overcrowding occurs in the network and it is a major concern of MANET. The control of congestion is the major trouble focused on mobile networks. To manage congestion means minimizing the traffic entering a communication network. To neglect congestion or linking disabilities of the in-between nodes as well as to enhance speed of transferring packets, the technique to control the congestion is applied widely. So many researches

P. Pandey · A. Barve (✉)
Oriental Institute of Science & Technology, Bhopal, India
e-mail: barve.atul@gmail.com

P. Pandey
e-mail: preetipandey940785@gmail.com

R. K. Shukla et al. (eds.), *Data, Engineering and Applications*,
https://doi.org/10.1007/978-981-13-6351-1_10

are done in this area that are intended for reduction of overcrowding from the network. This paper is focused on congestion minimization by using the concept of multi-track-based routing. It can be done by transport-layer technology.

The transport-layer technology has multiple data routing. It sends via many routes to the recipient node of the future that enhance congestion control, network performance in the way of an action then the data rate of the sender is also analyzed if the sender transmission rate is greater than the future node rate then the transmission rate is reduced based on the transport layer technology. Discovery of several routes between the different sender and receiver processes at an instance of discovery of only track is compatible with the multipath directive [1]. At MANET, you can tackle the prevailing problems such as portability, security, age of network, etc., through multi-track routing protocols [4, 5]. The protocol increases the delay, performance and provides balancing of the load over the traffic in MANET. Multi-track orientation has a few limitations.

1.1 Inefficient Route Discovery

Avoid some multiple track routing practices and in-between node redirecting response of the cache path to establish the link of separate paths. Therefore, the sender waits for a response to obtained from the receiver. Therefore, the discovery of the path carried out by multiple routing protocols needs more time.

1.2 Route Request Storm

It creates many demands through a multi-track interactive routing protocol. When the node requires duplicate applications to handle intermediate messages, there is the possibility of creating unnecessary packets over the network. These additional packets decrease the availability of bandwidth for transmission of data, delay of time increases in each packet transmission and utilize extra power to send and receive network. Because of the way the request routing propagates, it is complex to limit the deployment of unnecessary packets.

2 Intrusion Detection System

Intrusion is the set of actions that attempt to modify the privacy, integrity or availability. Intrusion Detection System (IDS) is an application that observes the network traffic and it informs to the system or network administrator when any abnormal actions are found. Intrusion detection requires a carefully selected arrangement of Bait and Trap. The task of IDS is to distract the attention of the intruder. IDS carries

out different tasks from which recognizing the intruder activity is the primary one. Various intrusion detection systems have been planned for wired network in which all traffic goes through the switches, routers or gateway so that IDS can be easily implemented on these devices. Whereas on the other hand, MANET does not include all such devices and any user can easily access it because of its open medium. Thus, the IDS technique on wired network cannot be preferred over MANET. IDS performs various tasks but the most important is recognizing the intruder activity.

The activities mainly focus on the analysis part to discover possible intrusions in the network by monitoring nodes and exploring the pattern of traffic passing. Accordingly, give response to the system. These activities are shown in Fig. 1. The rapid development of MANET increases the significance of security in the network. The central challenge with computer security is to develop systems, which have the ability to correctly identify an intrusion which represents potentially harmful activity. Thus, the purpose of IDS is like a special-purpose device to both detect and prevent the anomalies and also avoid illegal access of data. In the current scenario, users look for the complete security of data at any cost, since security of data become prime requirement for everyone. The new challenges need several modifications in existing IDS system so as to make better correlation of alarm; the prediction and detection of false detection rate should be low. In modern period, neural networks and genetic algorithms are using the modeling and resolving computational problems and also proved successful.

To improve the efficiency of intrusion detection system (IDS) these conditions must be followed:

i. The prediction and detection of false detection rate must be low.
ii. The success rate in intrusion detection systems must be high.

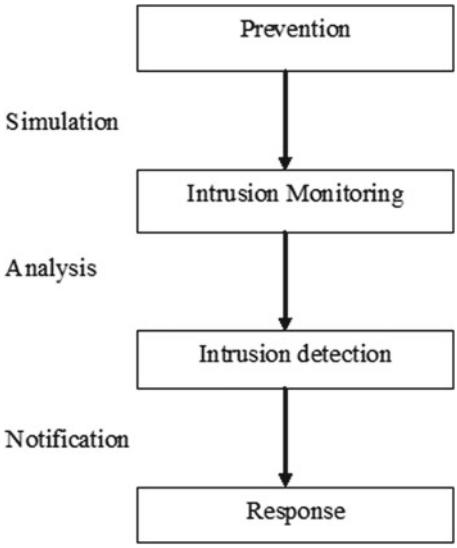

Fig. 1 Activities performed by IDS

iii. The residual energy should be as more as possible.
iv. The routing load must be low.

3 Related Work

This paper provides the pertinent on the presented effort in the area of protocol MANET orientation and congestion control. Many papers have been studied but some of them are presented here. The researchers as well as the intruder both have to understand the routing mechanism to defend or to fake the network. This means that the attacker applies the same type of attack on different protocols using different ways; and hence the researchers use different types of intrusion detection techniques on unusual routing protocols to guard against similar or dissimilar type of attacks. Ali and Huiqiang [1] Suggested Nkalpr, a protocol for dealing with load balancing in MANET. They used the basic structure and Oudw. In this approach, only delay in saliva packets over a fixed time is done and then transmitted. It also uses greeting messages periodic increases in addition to directing the public expenditure generated throughout the network. Liu et al [4] Combines the quality of multi-service mechanism of pregnancy restriction to discover the satisfactory link for a node and the predicted equilibrium scheme node. The key idea of researchers is to build up a load balancing. It can record every change in the case of the strategy of the biology of pregnancy and capable to decide methods loaded with the information of the situation surrounding pregnancy. Okougl protocol makes an extension in Oudw uses biodegradable information and loads network distribution loads of bandwidth nodes that may avoid the network to form the place of congestion, and neglect the power of node full of people who must wear out. Yi et al. [5] in the algorithm gain highly flexible and extend through the use of dissimilar link metrics and cost functions. The ring application detects process and restores the track in the MP-Ooser with the aim of increasing the quality of service with regard to Ooser system. It formulates multiple routing protocols for MANET routing, scalability, safety, time of networks, and the lack of transmission stability, and adaptation. Vijaya Lakshmi and Shoba Bindhu [6] suggested tailing mechanism and thus improve the network, such as the general productivity of network rules, and reduces the road delay, overhead and the possibility of traffic. And, this approach is created by directing the ad hoc network diagram. Narasimhan and Santhosh Baboo [7] proposed the development of hip-hop congestion using the routing protocol that uses the value of the guideline to measure the weight of routing combined, based on data rate, the delay in the queue, the quality of the link and Mac costs directly. Among the paths discovered, the path is selected with the minimum cost index, based on the load of every node within the network. Tawananh [8] developed congestion-control algorithm in the OTCBB multi-track power science, called Akmtkp. Ecosystems and transmits Internet Protocol traffic (Akmtkp) from more tracks to the more heavily loaded higher activity tracks, as well as from the top tracks the cost of energy to the lower tracks and improving the energy. Jingyuan Wang, Jiangtao Wen and others. In his work proposes a new algorithm to

control the congestion, called Tkvi that can lead safely in the wireless networks and of high AP. The algorithm of the parallel TCP program was inspired but with significant differences in the single contact without OTCBB a window and a jam of every TCP session, there are no changes in other layers (such as applications) layer in the system of a party in a party that needs to be done. This work was done only to control congestion transport by the method of improving the OTCBB layer but also congestion occurs in the direction of time thus work increases through congestion control technology base. Kai suggested Chen et al. [9] "Clear control based on the flow rate scheme (called Akestekt) MANET network." And correctly, the allowable transfer stream explicitly from the intermediate routers to terminate hosts in each particular control header in the packet data. Aksakt reacts rapidly and accurately to route and bandwidth difference, making it particularly appropriate for the dynamic network. Kazi Rahman suggested Chandereyma et al. [10] "Average-based congestion control explicitly (Ksark) for multi-media transmission in dedicated mobile networks." The Committee deals with TCP issues when engaged on dedicated networks, demonstrating a significant improvement in performance in the technical cooperation program. Although circa reduces the dropping of packets. It is caused via overcrowding compared to the OTCBB congestion control technique. He suggested Hong Qiang et al. [11] "a new control system on traffic from one party to other party" (Rbisk).

4 Game Theory

Neighbor discovery protocol (NDP) is mainly used for neighboring nodes discovery. Game theory is used to enhance security in mobile ad hoc network (MANET). Game theory helps in checking the reliability of neighbor node. Every node verifies its neighboring nodes that are within its communication range. This node stores the trust values of all verified nodes. Each node changes in a timely manner as per the trust parameter. After that nodes interchange the reliability rate with its corresponding neighbor nodes. Once the exchange process is done, if any specific node's successful transmission rate (trust value) is less than average successful transmission rate of network, then the node is declared as attacker. On the other hand, node which has greater successful transmission rate as compared to other transmission rates of network will be included as the member of the cluster.

$$\text{Reliability of node} = R \geq T$$

R is successful transmission rate of node.
T is average successful transmission rate of network.

5 K-Means Clustering

K-means is a technique used to divide the different patterns into various groups [7], if the data is categories in different patterns then n be the different types of patterns. Then the objective function is given by

$$\min S_w = \min \sum_{j=1}^{k} \sum_{i=1}^{n} a_{ij} \left\| Y_i - Z_j^2 \right\|. \tag{1}$$

Here, Y_i indicates the ith pattern and k be the number of clusters, $a_{ij} \in \{0, 1\}$ is cluster assignment, Z_j is the clustering point of the jth cluster and given by

$$Z_j = \sum\nolimits_{j=1}^{n} a_{ij} * Y_i / \sum\nolimits_{j=1}^{n} a_{ij} \tag{2}$$

where $\sum_{j=1}^{n} a_{ij} = 1$

When intra-cluster compactness is decreased then the objective function also minimizes. Suppose n samples are taken, pick k location as an original clustering center, next coming sample is allotted to its nearby center. Now calculate the average and the fitness cost of each cluster, again following this procedure until the results do not vary. The clusters have centroids, which are formed using K-means algorithm. It takes the input as the features of the nodes like total number of RREQ sent by each node or total number of RREP received by each node etc. K-means clustering having the initial clustering centers gives a grand outcome and become responsible toward the local optimum. Taking the outer node as the center of cluster is the wrong choice, besides, inter-cluster partition is not effectively used. In the next section of this paper, these problems are solved by constructing a new model. PSO algorithm is presented, to optimize this model.

6 Proposed Cluster-Based Game Theory

Various techniques have been projected to identify unauthorized user, misuse of systems by either insiders or external intruders. Due to the rapidly increasing unauthorized activities, Intrusion Detection System (IDS) as a component of defence-in-depth is very necessary because traditional technique is unable to supply total security from intrusion. Along with that, mobile nodes operate on the limited power of battery, therefore, it becomes very necessary to develop techniques which can successfully maintain lesser complexity. To maintain the mobile ad hoc network it is necessary to divide the whole network into small and different groups called cluster. Every cluster is different from the other. Such a network becomes more manageable.

Clustering is a technique which combines nodes to form a group. These groups in the network are known as clusters.

The main idea behind clustering algorithm is to first create and then maintain the cluster. The cluster should be capable of adding different nodes in the cluster according to the behavior. In most clustering techniques nodes are preferred to play different function according to a certain criteria.

According to different roles performed by the nodes, types of nodes are defined:

i. Member node: It is also called Ordinary node. This node is neither a Cluster Head nor the gateway node. Each member node belongs exclusively to cluster. They are free from their neighbors that might exist in a different cluster.
ii. Gateway: Nodes with inter-cluster links, these nodes are useful in forwarding the information between different clusters at the time of communication.
iii. Cluster Head: A node in a cluster which is associated to all the members of the cluster. There is only one cluster head in every group who controls all the activities of cluster.

6.1 Responsibility of Cluster Head

Cluster head maintains the activity of a group of nodes or cluster so that the communication can execute securely over the network. Cluster head is said to be trusted node. Cluster head is in charge for the overall management of its own cluster and also communicate with other clusters. A cluster head can communicate to the other by communicating its cluster head. If the outside node tries to communicate any node of the cluster then cluster head authenticates the outside node and then allow accordingly.

The cluster head selection may differ according to such factors like geographical position of the node, its stability, energy efficiency, trusted nodes, etc. Cluster Head node is a special mobile node with additional functions. Cluster head verifies the behavior of embedded nodes and if the previous records were verified then a certification is given to the node as shown in Fig. 2. As the new node entered to the cluster or any member node leaves the cluster head verify the authentication service.

Searching of new cluster head before time out on the basis of following parameter

i. New node should have minimum work load responsibility.
ii. New node should be easily reachable over cluster area.
iii. New node should be energy efficient.
iv. Existing cluster head hand overs their responsibility and remain the cluster head during swapping.

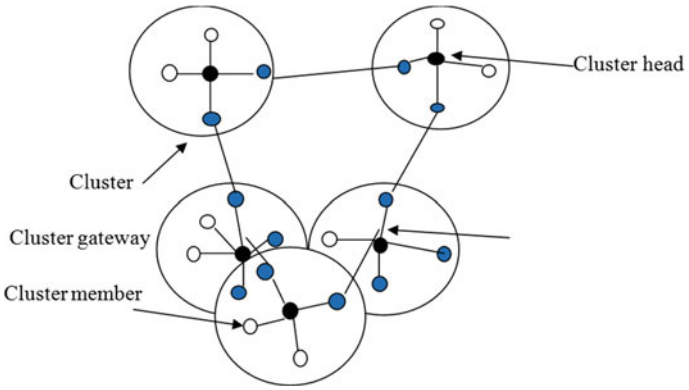

Fig. 2 Roles of nodes in cluster

6.2 Algorithm (Cluster Game Theory)

Assumption:
N^{i}_{MANET} = Mobile adhoc network having i mobile node
$M = \{X_i | X_i \text{is ith mobile node } \in N^{i}_{MANIT}\}$, Set of Mobile node
$NN^{Xi} = \{Y_i | Y_i \text{ is ith neighbour node of } X_{ith} \text{ mobile node } \in N^{i}_{MANIT}\}$
Algorithm:
{

Step 1: If any Source node (X_S) wants to communicate with their desired destination (X_D) then destination (X_D) authenticates the Source node (X_S)
Step 2: Initially Source node (X_S) send Hello packet to their destination (X_D)
Step 3: Destination (X_D) check whether Source node (X_S) belong to same cluster If yes Go to step 4 else go to step 5
Step 4: Destination (X_D) verifies and allows communication with Source node (X_S)
Step 5: Destination (X_D) forwards their hello packet to their cluster head (CH) to authenticate Source node (X_S)
Step 6: CH node applies game theory to authenticate Source node (X_S) via broadcasting authentication packet for Source node (X_S)
Step 7: If Source node (X_S) is successfully authenticated then it becomes the member of their cluster and go to step 3, otherwise regret the communication.

In this process, it is possible that one node becomes the member of one or more cluster and their communication system over respective cluster has been control by their cluster head. In the proposed work both inter-cluster and intra-cluster authentication is carried out with the help of cluster head (Fig. 3).

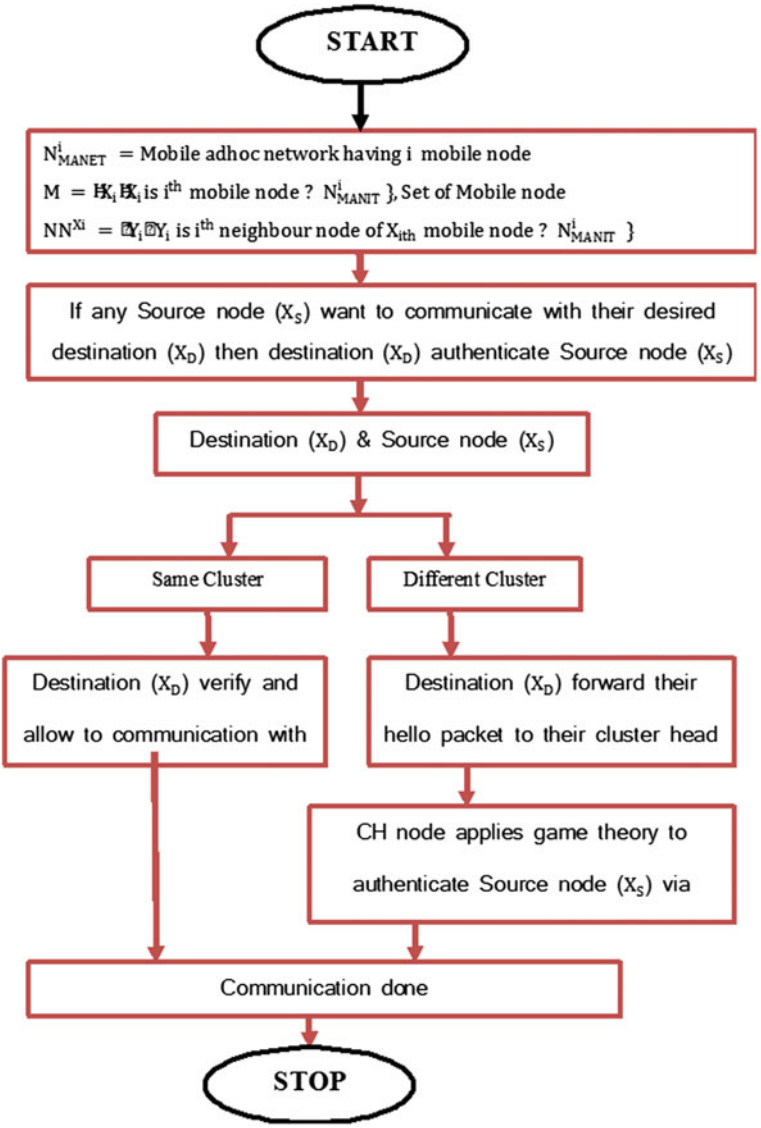

Fig. 3 Proposed flowchart

7 Result Analysis

Proposed methodology gives the better result in various factors. The factors are packet delivery ratio, battery power consumption, and control packet overhead.

7.1 True Detection Rate

Proposed methodology use K-means which return high TDR Rate as compared with existing approach by using Machine Learning Technique.

The working of an intrusion detection system is measured by TD (True Detection) rate and FD (False Detection rate) rate. If we calculate the ratio of strange patterns noticed by the system and the number of strange patterns then it will give TD rate.

Here A represent attack and I represent Intrusion

$$\text{TDR} = \text{P}\ (\text{A} \mid \text{I}) \tag{3}$$

Similarly, TD (True negative) rate can be calculated as

$$\text{TDR} = \text{P}\ (-\text{A} \mid \text{I}) \tag{4}$$

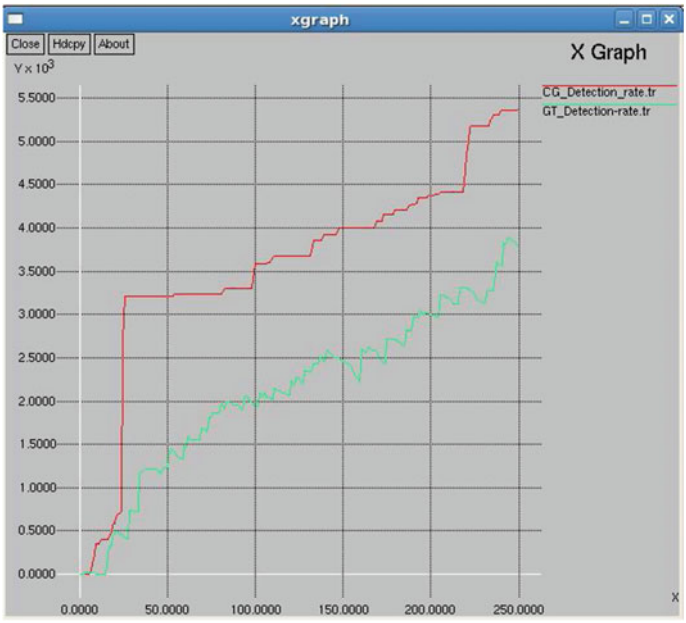

Fig. 4 True detection rate comparison

Figure 4 shown true detection rate here red line shows proposed method detection rate whereas green line shows existing method. For any efficient method, it is required to have higher true detection rate. As shown in Fig. 4 proposed methods having higher true detection rate.

7.2 False Detection Rate

It means if a system wrongly identifies the normal pattern as abnormal patterns. In this experiment, FD rate is written as the fraction of False Detection recognized by the system and total number of intrusion.

Figure 5 shows false detection rate where red line shows the proposed method detection rate, whereas green line shows existing method. For any efficient method, it is required to have lower false detection rate. As shown in Fig. 5, the proposed methods have lower false detection rate.

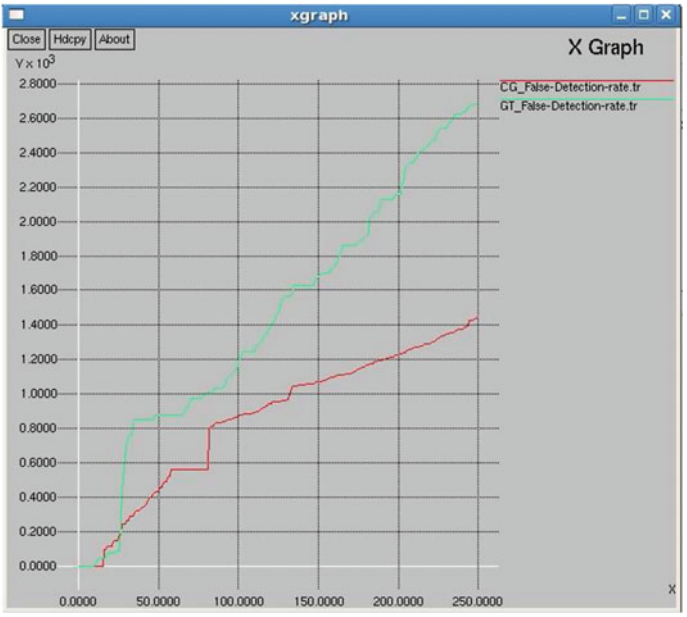

Fig. 5 False detection rate of the proposed protocol and existing protocol

7.3 Monitoring Node

For any ideal routing protocol, it is required that it has lower Monitoring Node, whereas existing approach by using Game Theory have required higher Routing as compare to proposed methodology by using Cluster-based IDS with AODV.

Figure 6 shows the Routing load where red line shows the proposed method of detection rate whereas green line shows the existing method. For any efficient method, it is required to have lower Routing load. As shown in Fig. 6, the proposed methods have lower routing load as compare to existing one.

7.4 Resident Energy

Energy saving routing protocol tries to move lower energy node towards less traffic and higher energy node towards high traffic and reduce retransmission whereas existing approach only minimized redundant path and increase Resident energy.

$$\text{Resident Energy} = \sum_{n=1}^{n=m} E_n - E(r_p + t_p + c_p) \tag{5}$$

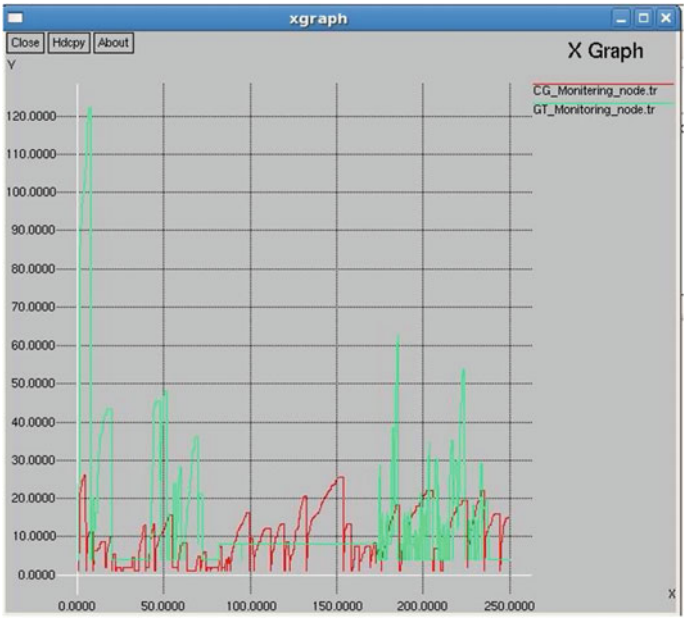

Fig. 6 Monitoring node of the proposed protocol and existing protocol

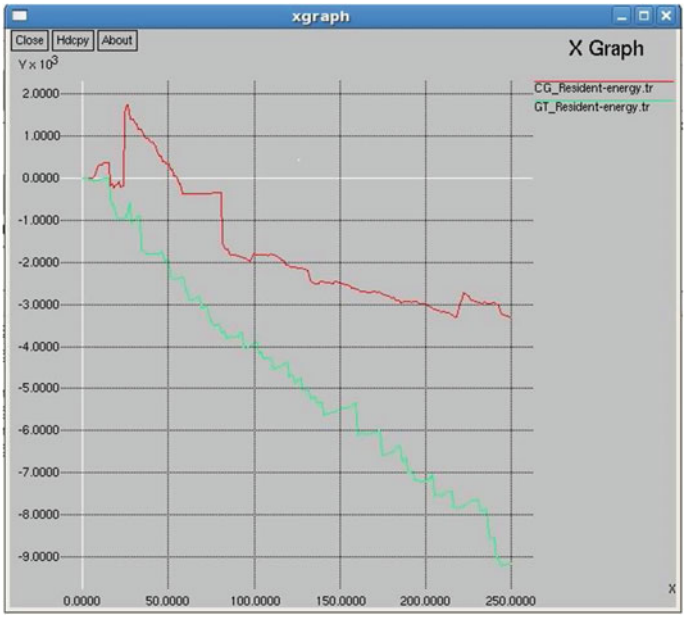

Fig. 7 Resident energy of network in the proposed protocol and existing protocol

where E_n = Intial Energy of Node N
where r_p = Number of recived packet via node N
where t_p = Number of transmit packet through node N
where c_p = Number of control packet through node N

Figure 7 shows resident energy of network where red line shows the proposed method detection rate, whereas green line shows the existing method. For any efficient method, it is required to have higher resident energy. As shown in Fig. 7 the proposed method have higher resident energy as compare to existing one.

8 Conclusion

This energy efficiency protocol paper play block proposed to guide IDS over network security in MANET. It has suggested different techniques, but there is a lack of power consumption. In order to overcome all these deficiencies proposed on the basis of game theory, it has been suggested for IDS that the integration of game theory and K-means. The methodology proposed uses the theory to calculate the degree of reliability in which the scope of K-means provides reliability to Cluster head of a specific mass. In future work, we can improve the theory of gaming, taking into account the standards related to quality of service and time. Here, in all proposed works, a homogeneous network is assumed in a way that all the nodes have the same

capacities in terms of their computational and energy resources. We wish to extend our model to support a heterogeneous network.

Reference

1. Ali, A., Huiqiang, W.: Node centric load balancing routing protocol for mobile ad-hoc networks. In: International Multiconference of Engineers Computer Scientists, IMECS 2012 Hong Kong, 12–16 Mar 2012
2. Reddy, A.V., Khan, K.U.R., Zaman, R.U.: A review of gateway load balancing strategies in integrated internet—MANET. In: IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA), Bangalore, India (2009)
3. Umredkar, S., Tamrakar, S.: Recent traffic allocation methods in MANET: a review. In: The Next Generation Information Technology Summit, Noida, 2013, pp. 220–226 (2013)
4. Liu, K., Liu, C., Li, L.: Research of QoS—aware routing protocol with load balancing for mobile ad hoc networks. In: 4th International Conference on Wireless communication (2008)
5. Yi, J., Adnane, A., David, S., Sterile, B.: Multipath optimized link state routing for mobile ad hoc networks. 28–47 (2011)
6. Vijaya Lakshmi, G., Shoba Bindhu, C.: Congestion control avoidance in ad hoc network using queuing model. Int. J. Comput. Technol. Appl. (IJCTA) **2**(4) (2011)
7. Narasimhan, B., Santhosh baboo, S.: A hop-by-hop congestion-aware routing protocol for heterogeneous mobile ad-hoc networks. Int. J. Comput. Sci. Inf. Secur. (2009)
8. Hong, C.S., Le, T.A., Abdur Razzaque, Md., et al.: An energy-aware congestion control algorithm for multipath TCP. IEEE Commun. Lett. **16** (2012)
9. Chen, K., Nahrstedt, K., Vaidya, N.: The utility of explicit rate-based flow control in mobile ad hoc networks. In: Proceeding of IEEE, Wireless Communications and Networking Conference (2004)
10. Hasan, S.F., Rahman, K.C.: Explicit rate-based congestion control for multimedia streaming over mobile ad hoc networks. Int. J. Electr. Comput. Sci. **10** (2010)
11. Fang, Y., Zhai, H., Chen, X.: Rate-based transport control for mobile ad hoc networks. In: IEEE Wireless Communications and Networking Conference, vol. 4 (2005)
12. Wang, J, Wen, J., et. al.: An improved TCP congestion control algorithm and its performance. IEEE (2011)
13. Indirani, G., Selvakumar, K.: A swarm-based efficient distributed intrusion detection system for Mobile ad hoc networks. Int. J. Parallel Emerg. Distrib. Syst. (2014)
14. Singh, S.K., Singh, M.P., Singh, D.K.: Routing protocols in wireless sensor networks—a survey. Int. J. Comput. Sci. Eng. Surv. **1** (2010)
15. Jangir, S.K., Hemrajani, N.: A comprehensive review on detection of wormhole attack in MANET. In: International Conference on ICT in Business Industry & Government, Indore (2016)
16. Singh, R.K., Nand, P.: Literature review of routing attacks in MANET. In: International Conference on Computing, Communication and Automation, 2016, pp. 525–530 (2016)

17. Wu, B., Wu, J., Chen, J., Cardei, M.: A survey on attacks and counter measures in mobile ad hoc networks. Springer, Wireless Network Security (2007)
18. Chaurasia, B.K., Tomar, G.S., Shrivastava, L., Bhadoria, S.S.: Secure congestion adaptive routing using group signature scheme. Springer Transaction on Computer Science, vol. 17, 2013, pp. 101–115 (2013)
19. Trivedi, A., Sharma, P.: An approach to defend against wormhole attack in ad hoc network using digital signature. IEEE, pp. 307–311 (2011)
20. Tomar, G.S., Shrivastava, L., Bhadauria, S.S.: Load balanced congestion adaptive routing for randomly distributed mobile ad hoc networks. Springer Int. J. Wirel. Pers. Commun. **75** (2014)