Energy Secured Intrusion Detection System and Analysis of Attacks for Mobile Ad-Hoc Networks

Rajendra Prasad P and Shivashankar
Department of Electronics & Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru and Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India
Email: {rajisvec, chenduss123}@gmail.com

Abstract—Mobile ad-hoc networks (MANETs) have drawing popularity due to its vast range of application in real time from all the researchers. The major concern in this type of networks is the security, as it lacks firewalls and sufficient software which fails to the data protection in ad hoc networks. The networks are prone to different types of attacks ranging from the selfish and malicious nodes. The challenges are to build the secured intrusion detection system (S-IDS) that provide security to nodes in the networks. Many intrusion detection systems have been implemented, which focuses on either routing protocols or their efficiency, but they do not address the security problems. In this proposed work, we aim to investigate the effect of independent attacks on dynamic source routing protocol and provide pseudo code for the different types of attacks. We observe the impact of each of the attacks on performance of the network by varying the number of malicious nodes in the network. The simulations are setup in network simulator-2 and the performance of these attacks against the proposed algorithm has been calculated and the results are analyzed with the existing dynamic source routing protocol under energy consumption, throughput, packet delivery ratio (PDR) and end-to-end delay as performance metric.

Index Terms—Mobile ad-hoc network, intrusion detection system, attacks, security

I. Introduction

Today, wireless communications and in particular Mobile Ad-Hoc Networks (MANETs) are self-configuring and pre-established infrastructure types of networks. Ad-Hoc networks are the spontaneous networks that provide communication everywhere for the mobile users and access the information regardless of location. The routing protocols in MANETs are designed assuming that no node in the network disrupts the proper functioning of the protocol, they fail to provide defense against attacks launched by any selfish and malicious nodes. The upcoming research field is more extreme on design of protocols for the efficient and prolongs battery life by addressing and providing the pseudo code for different types of attacks [1]-[4] for the existing routing protocol. All the mobility wireless devices are mainly operated on the limited battery power. The integration of improved computing and communication techniques has opened up many opportunities for development of ad-hoc networks. Diverse software and hardware designs have come up with distinctive requirements in applications but lacks in providing the security. Several design challenges in implementing and deploying of nodes to tackle these types of eaves drop and route invasion attacks in the real time. The protocol needs to overcome the attacks, for the improvement of network efficiency. The different types of attacks in the wireless network can be classified as selfish attacks and malicious attacks. The selfish attacks refer to node non-cooperation data transmission in the network. This non-cooperation from the nodes, primes to retransmit the data indeed in the system, accordingly devouring more energy of the nodes in the network. The malicious attacks refer to not following the protocol structure respectively in the network. A malicious attack is a compromised node which is purposely malicious [5].

As MANETs have high node mobility, interference and path loss, they have no stationary topology. Hence, they require a dynamic routing protocol for their proper functioning. The categorizations of the two types of routing protocol are:

A. Proactive Routing Protocol

In this protocol, the routing information is forwarded to all the neighboring nodes and the route information is spread all over the network and updated regularly. These routes are preserved irrespective of whether they are used or not, which results the availability of the path for nodes to transmit information any time in the network. The major drawback in this are network maintenance that results in relatively high network overhead and maintain route information at the expense of energy consumption.

B. Reactive Routing Protocol

In this protocol, the nodes find the routes to destination, only when data transmission is available, hence reactive routing protocol. These protocols are more suitable to the mobile ad-hoc network due to their ability and efficiency in adaptation to routing overhead. The drawbacks in these types of network are discovering paths from source to destination will introduce more delays [8], [9].

In this proposed work, the objective is to build a secured intrusion detection system for the nodes in reactive routing protocol to transmit information form source to destination and reducing the consumption of energy while transmitting. Also provide the pseudo code

Manuscript received September 25, 2019; revised April 3, 2020.
Corresponding author email: rajisvec@gmail.com
doi:10.12720/jcm.15.5.406-414

and investigate its performance for different types of attacks like black hole and route invasion particularly on existing DSR with the proposed protocol for Mobile Ad-Hoc Networks.

The structural flow of the proposed work is described as follows. The introduction section discussed the issues and challenges related to the MANETs in brief. Section II reviews the existing work related to the routing protocols, intrusion detection system and survey on different types of attacks. Section III provides the detailed description of the design and its implementation of the proposed algorithm. Section IV provides discussion on the simulation parameters and comparison analysis is done at the end of section. Finally, we conclude the result of the proposed work in the conclusion.

II. Related Work

The major related issues in mobile ad-hoc network are the route calculation and providing security to the nodes [5]. That deals to find the best and accurate route to the sink node during the mobility and network topological changes and uniformly distributed in the network. Researchers presents with the simple algorithm [6] implementation that describes, and which promises connectivity between the nodes, strong communication and stated node limitation to radio range wireless communication. There are many available existing protocols that are based on shortest route path protocol mechanism and flooding algorithm is used in the proposed system [7]. A dynamic routing algorithm is developed for possible elimination of the ideal links at the time of backbone network setup will not yield minimum energy solution for route calculation to establish and maintain the network for connection related sessions which make use of the knowledge of re-routing configuration to cope with the nondeterministic topology changes [8]. The shortest path routing algorithms are used in MANETs in order to know the number of hops is the path length of the routing protocols [9].

The security issues in mobile ad-hoc network needs to be addressed by building secured intrusion detection system that addresses issues related to the secured path to the nodes for data transmission, minimum node energy consumption and to develop security schemes that can deal with selfish and malicious nodes in the network.

For a wireless radio spectrum to communicate in a mobile network, MANETs differ significantly from other existing networks and co-operative network. The mobile nodes are dynamic in nature and also act as administration in the network topology [9]. These nodes are self-configuring and intended to be de-centralized control in the network topology. In such networks, it is not desirable to assume all the nodes will have single hop communication with each other. So, such type of networks need specialized efficient routing protocols which provide self-starting behavior of mobility. In such situations, existing wired network routing protocols would degrades in performance. In wireless correspondence framework, there is dependably interest for new routing protocols have been on interest in MANETs. Invention of any new wireless routing protocol is classified based on the mobility and character in which route tables are created, maintained and updated [10]. Network performance based on battery power has been major focusing area for research on routing protocols in MANETs. The designed conservative routing algorithms in [11] which are performance based and optimization fairly power efficiency. For multi-hop communication various routing protocols have been proposed [12]. These protocols, traditionally evaluated in terms of data rate loss, packet overhead and route length. A growing emphasis on long-lived networks has added energy consumption as an important metric. A number of research studies have been done on energy routing protocols of MANETs. These are the main challenges issues in wireless communication. All these problems including reliable energy consumption and gaining accurate spectrum are considered in the earlier research work.

The paper [13] presents the implementation of DSR and ZRP for secure intrusion detection system and provided the codes for different attacks. Their results showed that these attacks degraded the performance of the routing protocols quite significantly.

In [14], the paper discussed the effects of the malicious attacks related to the black hole and flooding implemented on AODV. The performance metric considered in this paper are Packet Delivery Ratio, Average End-to-End Delay and Normalized Routing Load. The effects of the black hole have impacted on the less packet delivery ratio. The flooding attack increases the normalized routing load.

The paper [15] argued the effects of different attacks which results in high routing overhead leading to the low throughput of the network performance.

The authors [16] analyzed the performance of network with malicious black hole nodes under DSR protocol using OPNET Simulator by varying the number of black hole nodes in the network. The results showed that the network performance deteriorates with the increase in the number of black hole nodes.

Many researchers have focused issues related to secure routing path that uses minimum energy for its transmission and also discussed security concern for it, but these are not efficient and fails when dealing with the different types of attacks in the real time. Such defense mechanisms can be developed only with the extensive knowledge of these attacks. Hence, in our proposed work, a defensive mechanism must be developed that deals with different types of attacks and their impacts has been analyzed.

III. Intrusion Detection System In Routing Protocol

Intrusion detection system schemes for the mobile ad-hoc network have not been implemented completely. The

S-IDS algorithm differs in the infrastructure and architecture compared to the wired networks and wireless networks [17]. In mobile ad-hoc networks, as there is no infrastructure, it's tranquil for the node attacks in the networks causing threatening challenges design requirement of the S-IDS. In the mobile ad-hoc network, the nodes move freely in the network, which allows one or more nodes to be captured and comprised in the network. The S-IDS results high efficiency only when all the nodes in the network co-operate in data transmission and the algorithm prevents attacks generated from the malicious nodes. The S-IDS algorithm regularly updates the node information to safeguard the nodes in the network. The different routing algorithm in MANETs like DSR, AODV and ZRP has been discussed.

A. *Dynamic Source Routing Protocol*

In dynamic source routing (DSR) protocol, the protocol find the shortest path, when the source node wants to transmit information to the destination node. In this protocol, the broadcasting of messages is limited by not sending frequently messages in the network and providing less overhead. It uses route cache to react instantly when route failure occurs [18].

B. *Ad-Hoc on-Demand Distance Vector Protocol*

The routing path information in the Ad-hoc on demand distance vector (AODV) protocol starts from the source to destination is generated by minimizing number of required broadcasts messages, as it creates route path on the basis on demand in the network. In this, the protocol uses group of messages such as Route Request (RREQ), Route Reply (RREP) for creating the route path in the network.

C. *Zone Routing Protocol*

In this zone routing protocol (ZRP), the nodes generates the route path by examining the nodes availability in the particular zone, if not then the route path establishment is not possible. These types of protocol are suitable for mid-range types of networks [19].

In the proposed protocol, the existing DSR protocol is been modified by including secure intrusion detection system and analysis of the protocol for black hole and denial of service attacks. The secured intrusion detection systems are considered to be essential in determining the network efficiency and providing network security to the network. Designing a secured intrusion detection system for mobile ad-hoc network and providing pseudo code for black hole and route invasion attacks are implemented in the proposed work.

IV. Design Of Proposed Algorithm

Dynamic source routing protocol establishes the route path, beginning from the source node to its destination node by broadcasting a set of messages in the network, when required by the source. Using a connection establishment process, the necessary path will be obtained by the nodes, as and when required. The stack wherein the diverse layer of the network protocol are focused in order to have better efficiency and different regressive practices have begun in the area of power conservation. On the other hand, the MAC layer and the network layer have been focused for the examination.

In the proposed work, the consumption of node energy in MANET is been divided into 3 categories: (i) energy utilized for transmitting data packets, (ii) energy utilized for receiving packets and (iii) energy utilized in idle state. The energy optimization cannot be achieved if there is MANET overhearing. The energy expended for the gathering and transmission of parcels is the fundamental center of this paper and the idle state energy loss.

A. *Route Discovery Mechanism in Proposed Algorithm*

The source node sends RREQ parcel when it does not have one accessible and cravings a route to a destination [20]. Every one of the nodes other than destination node ascertains the expense of the connection and afterward they include it in the RREQ's header. In the event that the node is middle of the nodes rejects the RREQ or on the off chance that it is the destination node, then it gets all the RREQ with the identical telecast ID and source IP Address. The clock starts at the paramount RREQ to the destination hub and is the same clock for all the RREQs with the same source address and telecast ID. This is the point out as the destination node may get RREQs from different sources or other telecast ID in the meantime. Subsequently, destination has differing clocks for each one of a kind RREQ. RREQ is received at the destination, checks if it's already heard it earlier, if it is not heard earlier, then it initiates timer, which records the cost link of the route with minimum cost in the list.

If additional RREQs arrival is present with the similar Broadcast ID and source address, then the minimum cost is compared to the new RREQ cost packet.

The cost is modified to the new minimum one, if new packet arrives that has less cost, then the information related to the route will be stored in the RREQ. But if the new RREQ cost is higher, then it is retained with previous information, i.e., nothing will be changed.

At that point when the time terminates, the destination node sends REPLY subsequent and to put away the RREQ with lower connection cost. When the first RREQ is received, in the existing reactive protocol the destination generates RREP. So the briefest course is picked and the various RREQs are disposed. The proposed algorithm can have the privilege of choosing the route that in light metric of energy-aware.

The step involved in multiple route discovery paths in the proposed algorithm is given below

- Node deployment in random
- Selection of source node, destination node and various network parameters
- Find the neighbor nodes (N)
- Start from the first node till all the neighbor nodes
- Perform Individual route discovery using E S-IDS routing protocol between source node and destination node.

- Cache the route
- Repeat process until all routes are found.

To have a better understanding of the routing protocol of proposed work, Fig. 1 shows the route discovery selection based on the minimize energy consumption and minimize cost.

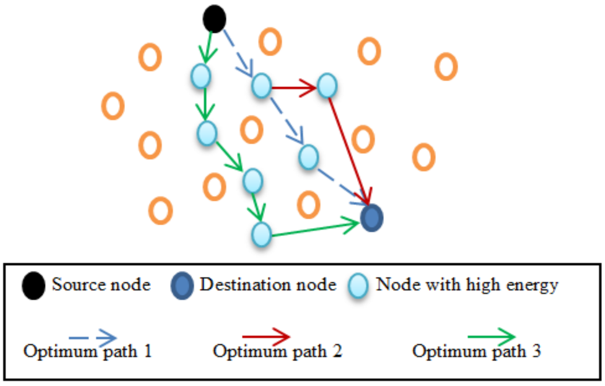

Fig. 1. Route discovery in proposed algorithm

The source node sends RREQ to its neighboring node in the network to collect information regarding the availability of node energy and rout path to the destination. Then the source nodes receives RREP from the others nodes to join the network and the process continues till all the nodes in the network completed.

B. Minimize Energy Consumed per Broadcast

Energy consumption is one of a most indisputable metrics which throw back our immediate insight roughly safeguarding energy [21]. Define l as few packets to broadcast in the networks in which to pass or move over the number of nodes $n_1, n_2, n_3, \dots, n_k$ where n_1 is considered as the source and $n_2, n_3, \dots, n_k$ are neighbor/intermediate nodes that retransmit this packet. $T(n_i)$ is the power consumption by the node n for transmitting total number of data packets. Then the energy consumed for packet l by all the transmitters is given as equation (1)

$$E_l = \sum_{i=1}^{k} T(n_i) \tag{1}$$

Thus, the desire about metric is to reduce E_l, for all broadcast packets l. It is not difficult to manage the metric that will cut the respectable energy consumed per broadcast packet. It is also not difficult to manage the metric that also will cut the respectable energy consumed per broadcast packet. However, it is not inconsequential to get ahead this metric as it is esoteric to engage the proficient broadcast trees to get ahead this goal. One major drawback the metric have is that the nodes will toil to have frequently divergent energy consumption profiles which could authorize in promptly demise for sprinkling nodes.

C. Minimize Cost per Packet

For maximizing the all career node functions of networks, previously metrics distinctive than desire consumed by each packet require to be used. The paths engaged when by the agency of these metrics should be a well-known that nodes with depleted energy reserves do not become intermediate nodes on multiple broadcast trees [22]. Let the node cost is denoted by $f_i(x_i)$ which denotes the weight of node i,x_i represents the total energy by means of this far. The charge per cost of transmitting a packet l from source n_l to all nodes going through intermediate nodes $n_2, \dots, n_k$ is given by equation (2),

$$C_l = \sum_{i=1}^{k} f_i(x_i) \tag{2}$$

The desire about metric is to minimize C_l and abode of packets l. Subliminally, f_i denotes a node's reluctance to earlier packets and we boot see that by all of a suitably chosen f_i, we can accomplish a different goals. In this way, if f_i is a monotone collective work, nodes that lie on many trees will not be completely used herewith accumulative their life. Conversely, the delay and the energy consumed per packet make out are in a superior way for several packets. Here, f_i can further be tailored to strongly reveal a battery's exclusive lifetime. Many batteries bring to light a discharge curve which lessens faster than linearly by all of increased use. So, it can behave two f_i's, linear and quadratic, in crucial the cost to ahead a packet over a node.

We can summarize small number of the benefits of this metric as:

- It is accessible to relate the battery characteristics soon into the broadcast protocol,
- Effects of network congestion are undivided into this metric (as an increase in node cost right to contention).

V. Attacks on Mobile Ad-Hoc Network

A. Black Hole Attack

In this, the malicious node behaves normally during the routing process while it behaves abnormally during the forwarding.

To illustrate the understanding of the routing protocol in the presence of the black hole attack, Fig. 2 provides the route discovery from source to destination with 3 optimum paths as discussed in previous section.

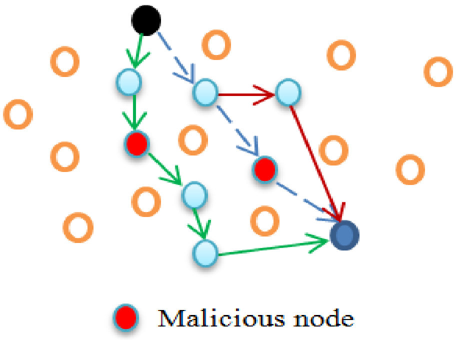

Fig. 2. Detecting malicious nodes.

The source node sends the RREQ messages to all its neighboring nodes for the route path. The malicious node also replies to source node with the RREP thereby dropping all the other nodes messages. The malicious node disrupts the communication which affects the network performance.

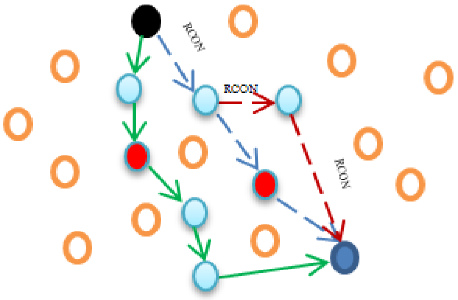

Fig. 3. Removing malicious nodes.

The energy secured intrusion detection system routing protocol protect the black hole attacks. Fig. 3 illustrate the protection, during the RREQ and RREP messages between the source and destination, nodes builds the route path and communicates with a unique response each time they transmit information, while the malicious node response to this transmission will always remain same for all type of communication in the network [23]. According to the proposed protocol, the entire nodes route establishment will be initially in waiting state, and once the source node confirms the selection of nodes, it transmits with a RCON message to its neighbor node to build the route path establishment till it reaches to the destination node. The route path also measures the availability of the energy till it reaches the destination node in the network.

B. *Denial of Service Attack*

In this attack, it prevents the availability of the network services to the nodes present in the network [24], [25]. This denial of service by the nodes is generally categorized as flooding affecting the network resources such as bandwidth, memory etc.

Flooding affects the nodes processing speed and the attacker will continuously transmits packets to the node and overhead the network. This affects the node performance in transmission regularly [26]. This degrades the network performance.

Considering the above attacks and its affects towards the performance of the network, and the protection of these attacks in the intrusion detection system have been implemented in the proposed work.

VI. Implementation of the Energy Secured Intrusion Detection System

A. *Energy saving Mechanism*

Without a fixed infrastructure, ad hoc networks have to rely on portable with limited battery power. In communication, the energy consumption at the node energy is dominant when compared to the energy consumption in processing. Thus the communication system must have efficient energy to optimize the different states consumption communication. The following sections briefly discuss energy models and some important techniques that used to design energy efficient routing protocols related with transmission power control and load balancing.

- Energy routing: here the transmission energy decides the routing, that is again depended on the distance from source to destination.
- Cost aware routing: here the lifetime remained is utilized as a metric for decision making.
- Combined energy and cost aware metrics: here both the energy of transmission along with node lifetime are combined in a link for cost computation and then use this as a metric to process.

B. *Mathematical Model of the Proposed Protocol*

Consider the appearance of the several packet l traverses nodes $\mathrm{n_1, n_2, n_3, \dots, n_k}$ where $\mathrm{n_l}$ is the source and $\mathrm{n_k}$ is the destination. The vitality expended is demonstrated by $\mathrm{T(a, b)}$ for accepting and transmitting a parcel around a hop from a to b. At that point the energy used for packet l is

$$E_j = \sum_{i=1}^{k-1} T(n_i, n_{i+1}) \tag{3}$$

Thus, the idea about metric is to, reduce $\mathrm{E_j}$ for all packets l. Under light loads, the routes chosen by this metric will be equivalent to routes occupied by shortest-hop routing.

If we adopt that $\mathrm{T(a, b)} = \mathrm{T(constant)}, \forall \mathrm{(a, b)} \in \mathrm{E}$, by the time mentioned the energy consumed is $\mathrm{T(k_l)}$.

To minimize the above, we simply need to decrease the valve k which is related as shortest hop routing. The ways chose by this metric are not evermore same as that of briefest hop routing. The measure of energy exhausted in transmitting one bundle totally over one hop will not be a constant considering consume of variable amounts of battery energy on contention [28]. Thus, in this situation the metric will inclined to route packets everywhere in congested areas. One profession weakness of this metric is that hubs will slope to have generally shifting energy utilization profiles bringing about straightforwardly death for some nodes. It prompts bigger utilization of power in the system. Some difficult situation in implementing this metric are

- Since nodes in dissimilar partitions independently capture routing decisions, we cannot accomplish the worldwide equalization required to expand the network partition time interim minimizing the normal postponement.
- Energy utilization is relying upon the length of the bundle, we cannot represent optimal routes without the development of future packet arrivals.

C. *Energy Secured Intrusion Detection System Routing Protocol for Mobile Ad-Hoc Networks*

The proposed protocol SERP implementation is given as follows:

Energy Secured Intrusion Detection System Routing Protocol for Mobile Ad-Hoc Networks

```
ES-IDS for MANETs()
//Initialize (create initial vectors for the nodes)
for (y=1 to N)
{
    if (y is the Source Node)
    {
        Route_Path [y] = Source Node
    }
    else if (y is a neighbor)
        Route_Path [y] = Source node + Neighbor node(measure energy level)
    else
        Route_Path [y]= empty
}
Send vector  RCON to the {Route_Path [1], Route_Path [2], .................., Route_Path [N]} to all neighbor node
//Update (improve the vector with the vector received from a neighbor)
Repeat (forever)
{
    wait (for a vector Route_Path  from a neighbor node)
    for (y=1 to N)
    {
        if (Route_Path includes Source Node)
            Discard the path
        else
            Route_Path [y] = Route { Route_Path [y], (Source Node + Route_Path [y])}
    }
    if (there is a change in the path)
        Send vector RCON to the {Route_Path [1], Route_Path[2] .....,Route_Path [N]} to all neighbor node
}
```

VII. Result and Disscussion

The implementation of the proposed work are evaluated on the varying performance i.e., with attacks and without attacks. The results are compared with the existing DSR protocol and the performance is measured in terms of energy consumption, throughput, packet delivery ratio (PDR) and end-to-end delay [29].

The experiments are implemented in network simulator-2 2.34 and the network field of simulator consisting of 50 nodes that are randomly distributed over the size of 500m * 500m area as shown in Fig. 4.

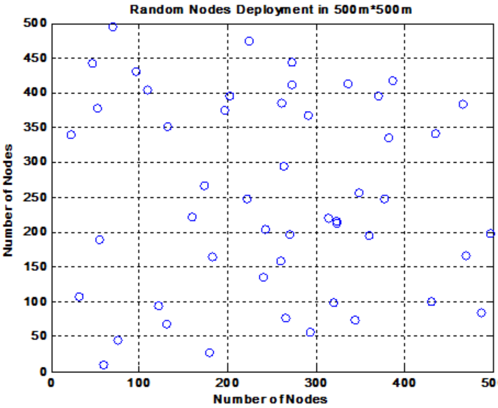

Fig. 4. Deployment of nodes.

As discussed in Section V, the black hole attacks drops the received packets and does not forward its packet for its associate nodes for communication in the routing process, it behaves maliciously in the routing process. This attack ordinarily behaves for the duration of the routing process to avoid detection and once available behaves maliciously in the network and drops the packets. Therefore, the conducted experiment for the attacks has been implemented in the network simulator-2. The simulation configuration parameters for implementation of the above said attacks are available in Table I. After setting up the configuration, the experiment are executed to measure the performance of the ES-IDS routing protocol against the DSR protocol.

Table I: Simulation Configuration Parameters

Parameters	Simulation Configuration
Packet Size	1000
Traffic Type	CBR
Antenna model	Omni antenna
Physical Layer S-Propagation	Two-ray ground
MAC Protocol	802.11
Queue Type	Drop Tail
Queue Size	50
NS-2 version	2.34
Bandwidth	1MB

The experiments are performed to evaluate the performance metrics in terms of the throughput, energy consumption, end-to-end delay and packet delivery ratio. The first experiment implementing the protocol under the no attack scenario and the result of the throughput under this is better in all the protocol as shown in Fig. 5. The results had shown almost uniform throughout for both protocols.

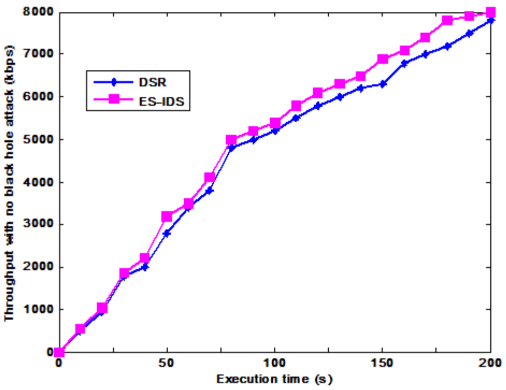

Fig. 5. Throughput with no black hole attack.

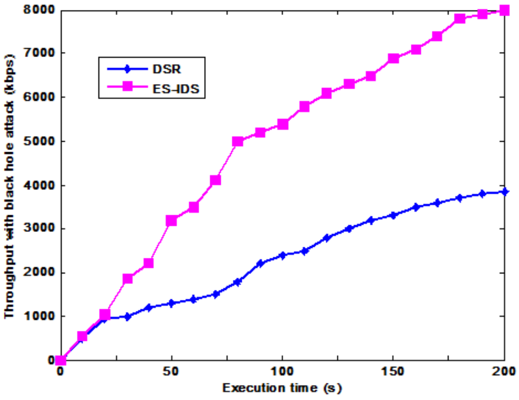

Fig. 6. Throughput with black hole attack

In the next scenario, the experiment implemented in the presence of the black hole attack by malicious node during the routing. The results of the throughput under this black hole attack performed with 2 malicious nodes considerably decreases in the existing DSR protocol but slightly reduce throughput when compared to the proposed ES-IDS as shown in Fig. 6.

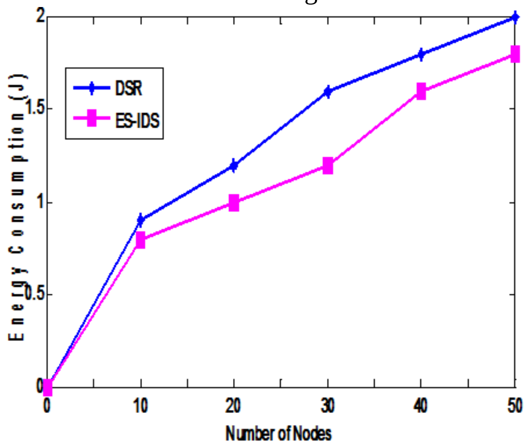

Fig. 7. Energy Consumption.

The total energy consumption is 68Joules of all the nodes for the duration of 200 seconds in the proposed ES-IDS routing protocol against the existing DSR protocol of 85Joules as shown in Fig. 7.

The observation showed reduction in consumption of energy and that can be utilized in the network for increasing the lifetime of the network.

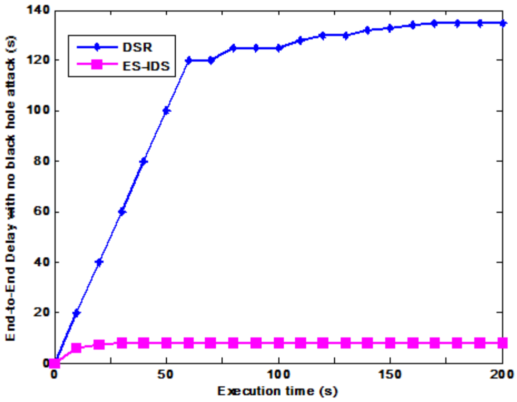

Fig. 8. End-to-End Delay with no black hole attack.

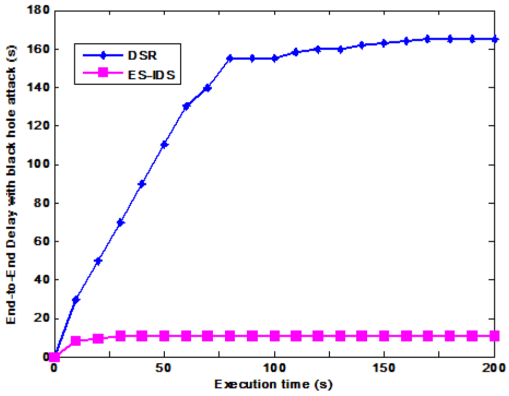

Fig. 9. End-to-End Delay with black hole attack.

The experiment visualizes the end-to-end delay under both the with black hole attack and with no black hole attack conditions of the two protocols to just give an indication about the overhead present in the network. Fig. 8 and Fig. 9 shows the end-to-end delay of the protocols under both cases is almost same. Results show proposed ES-IDS routing protocol experiences low end-to-end delay when compared to DSR protocol.

The packet delivery ratio under the no black hole attacks and with black hole attacks in both protocols have considerable effects as shown in Fig. 10 and Fig. 11. The packet drop is high in the DSR protocol compared with the proposed ES-IDS protocol.

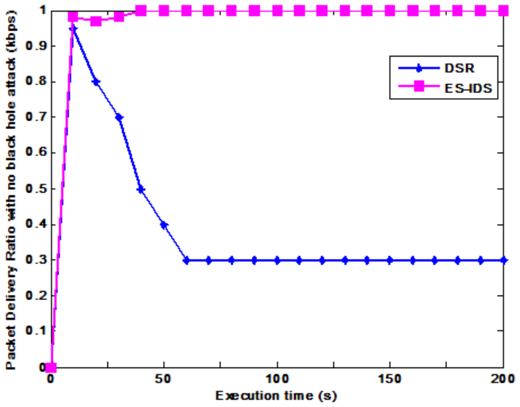

Fig. 10. Packet delivery ratio with no black hole attack.

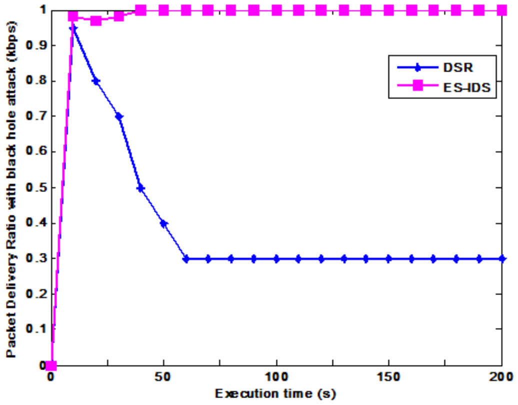

Fig. 11. Packet delivery ratio with black hole attack.

From the results of the simulation obtained in Fig. 5 to Fig. 10, we evaluate that the DSR protocol has a very good performance under attack free against compared with attacks. Also the ES-IDS protocol performs better under both scenarios of attacks generated by two malicious nodes.

Finally the results validate that the ES-IDS protocol exhibits better performance in the metrics considered during no attack and with attacks.

VIII. Conclusion and Future Enhancement

The paper introduced the energy secured intrusion detection system routing protocol for mobile ad-hoc networks The proposed protocol is implemented using the network simulator-2 and the protocol addressed the issues related to the routing, energy utilization, security constrained and addressed the different types of attacks in the network. In addition, it provided to protect against cooperative black hole attack that is performed by two malicious nodes that behave normally during the routing process but maliciously during the forwarding process. The analysis is performed with the black hole attack and the denial of service attacks and compared against the existing DSR protocol. The analysis of the protocol, and experimental result showed the better performance.

The future enhancement of the proposed work can be worked in presence of different types of attacks in different scenarios with increased number of nodes that can be implemented and providing secure transmission in the mobile ad-hoc network.

ACKNOWLEDGMENT

We gratefully thank Sri Venkateshwara College of and Engineering, Bengaluru and Visvesvaraya Technological University, Jnana Sangama, Belagavi-590018.

REFERENCES

[1] S. Prakash and A. Swaroop, "A brief survey of black hole detection and avoidance for ZRP protocol in MANETs," in *Proc. Int. Conf. Comput., Commun. Automat. (ICCCA)*, Noida, India, Apr. 2016, pp. 651_654.

[2] Z. Wang, Y. Chen, and C. Li, "PSR: A lightweight proactive source routing protocol for mobile ad hoc networks," IEEE Trans. Veh. Technol., vol. 63, no. 2, pp. 859_868, Feb. 2014.

[3] S. Kalita, B. Sharma, and U. Sharma, "Attacks and countermeasures in mobile ad hoc network_An analysis," *Int. J. Adv. Comput. Theory Eng*., vol. 4, no. 3, pp. 16_21, 2015.

[4] M. C. Trivedi, S. Yadav, and V. K. Singh, "Securing ZRP routing protocol against DDoS attack in mobile ad hoc network," in *Advances in Data and Information Sciences (Lecture Notes in Networks and Systems)*, vol. 39, Eds. Singapore: Springer, 2019, pp. 387-396.

[5] M. Hussain and A. Devaraj, "Upshot of sinkhole attack in DSR routing protocol based MANET," *Int. J. Eng. Res. Appl.*, vol. 3, no. 2, pp. 1737-1741, 2013.

[6] E. O. Ochola, L. F. Mejaele, M. M. Eloff, and J. A. van der Poll, "Manet reactive routing protocols node mobility variation effect in analysing the impact of black hole attack," *SAIEE Afr. Res. J.*, vol. 108, no. 2, pp. 80-92, Jun. 2017.

[7] M. A. Abdelshafy and P. J. B. King, "Resisting blackhole attacks on MANETs," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2016, pp. 1048-1053.

[8] G. Xu, C. Borcea, and L. Iftode, "A policy enforcing mechanism for trusted ad hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp. 1-15, 2011.

[9] Y. C. Hu, A. Perrig, and D. B. J. Ariadne, "A secure on-demand routing protocol for ad hoc networks," in *Proc. International Conference on Mobile Computing and Networking*, Atlanta, USA, 2012, pp. 12-23.

[10] J. Xiong, J. Zhao, and L. Xuan, "Research on the combining of compressed sensing and network coding in the wireless sensor network," *Journal of Theory Appl Inf Technol.*, vol. 47, no. 3, 2015.

[11] S. Olariu, Q. Xu, and A. Zomaya, "An energy-efficient self- organization protocol for wireless sensor networks," in *Proc. IEEE Intelligent Sensors, Sensor Networks, and Information Processing Conf.*, Dec. 2014, pp. 55-60.

[12] B. Krishnamachari, D. Estrin, and S. B. Wicker, "The impact of data aggregation in wireless sensor networks," *Distributed Computing Systems*, pp. 575-578, 2013.

[13] E. F. Nakamura, H. S. Ramos, L. A. Villas, A. de Aquino, and A. Loureiro, "Reactive role assignment for data routing in event-based wireless sensor networks," *Computer Networks*, March 2017.

[14] S. Basagni, M. Y. Naderi, C. Petrioli, and D. Spenza, "Wireless sensor networks with energy harvesting," in *Proc. IEEE International Congress on Ultra Modern Telecommunications*, 2016.

[15] D. P. Grawal and A. Manjeshwar, "A protocol for enhanced efficiency in wireless sensor networks," in *Proc. 15th Parallel and Distributed Processing Symposium*, San Francisco: IEEE Computer Society, 2015.

[16] O. O. Ekabua and I. Njini, "Genetic algorithm based energy efficient optimization strategies in wireless sensor networks: A survey," *Advances in Computer Science: An International Journal*, vol. 3, no. 5, no. 11, 2014.

[17] S. Z. Erdogan and S. Bayrakli, "Genetic Algorithm Based Energy Efficient Clusters (GABEEC) in wireless sensor networks," *Procedia Computer Science*, 2015.

[18] V. K. Arora and D. Prabha, "A survey on LEACH and its descendant protocols in wireless sensor network," in *Proc. International Conference on Communication, Computing & Systems*, 2014.

[19] S. Hamalainen, H. Sanneck, and C. Sartori, *LTE Self-Organizing Networks (SON): Network Management Automation for Operational Efficiency*, John Wiley & Sons, 2015.

[20] P. R. Prasad and Shivashankar, "Improvement of battery lifetime of mobility devices using efficient routing algorithm," *Asian Journal of Engineering Technology and Applications*, pp. 13-20, 2017.

[21] K. N. S. Kumar, P. R. Prasad, Shivashankar, S. S. Kumar, and R. Gatti, "Opportunistic routing technique for minimized energy consumption for relay node selection in wireless sensor networks," in *Proc. IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, 2016, pp. 2093-2097.

[22] S. H. H. Nazhad, M. Shojafar, S. Shamshirband, and M. Conti, "An efficient routing protocol for the QoS support of large ‐ scale MANETs," *Int. J Commun. Syst.*, 2018.

[23] Z. Guo, I. G. Harris, L. Tsaur, and X. Chen, "An on-demand scatternet formation and multi-hop routing protocol for BLE-based wireless sensor networks," in *Proc. IEEE Wireless Communications and Networking Conference*, New Orleans, LA, 2015, pp. 1590-1595.

[24] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function," *IEEE Access*, vol. 5, pp. 10369-10381, 2017.

[25] S. K. Das and S. Tripathi, "Energy efficient routing protocol for MANET based on vague set measurement technique," *Procedia Computer Science*, vol. 58, pp. 348-355, 2015.

[26] V. V. Mandhare, V. R. Thool, and R. R. Manthalkar, "QoS Routing enhancement using metaheuristic approach in mobile ad-hoc network," *Computer Networks*, vol. 110, pp. 180-191, 2016.

[27] S. Sarkar and R. Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks," *Ad Hoc Networks*, vol. 37, no. 2, pp. 209-227, 2016.

[28] W. Kuo and S. Chu, "Energy efficiency optimization for mobile ad hoc networks," *IEEE Access*, vol. 4, pp. 928-940, 2016.

[29] B. M. C. Silva, J. J. P. C. Rodrigues, N. Kumar, and G. Han, "Cooperative strategies for challenged networks and applications: A survey," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2749-2760, Dec. 2017.

[30] P. R. Prasad and D. Shivashankar, "Secured intrusion detection system energy routing protocol for mobile ad-hoc network," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1S6, pp. 32-37, December 2019.

[31] F. D. Tolba and P. Lorenz, "Multi path routing based energy-efficient for extending mobile wireless sensor networks lifetime," *Journal of Communications*, vol. 14, no. 12, pp. 1224-1228, 2019.

[32] A. Mouiz, A. Badri, A. Baghdad, and A. Sahel, "Analysis of energy consumption and evaluation of metric parameters of routing protocols in ad hoc (MANET) networks using: NS2 simulator," *Journal of Communications*, vol. 14, no. 11, pp. 1067-1074, 2019.

Rajendra Prasad P was born in India, in 1986. He received the B.E and M-Tech degree from Visvesvaraya Technological University, Jnana Sangama, Belagavi in 2008 and 2010 respectively and now pursuing the Ph.D in the wireless communication in Visvesvaraya Technological University, Jnana Sangama, Belagavi. Since 2011, he has working as an Assistant Professor in the Department of Electronics & Communication Engineering at Sri Venkateshwara College of Engineering, Bengaluru. He is the author of the several articles published in International/National Journals and conferences. His current interest includes wireless network, communication, mobile ad-hoc networks, security. He is also a reviewer for several journals and conferences.

Shivashankar was born in India, in 1979. He received the Ph.D degree from Visvesvaraya Technological University, Jnana Sangama, Belagavi in 2014. His Specialization is in wireless communication and research interest includes Focus on Wireless Ad Hoc & Sensor Networks and Cognitive Radio with emphasis on Design & Analysis of MAC and Routing Protocols. Cross Layer Design and Cooperative Diversity Schemes to Design & Analysis of MAC and Routing Protocols. He has received DST/AICTE/VGST/KSCST project funds. He is also the EXECOM MEMBER IEEE COMPUTER SOCIETY. His research publication includes in the reputed journal/transaction and conferences. Presently working as Professor and Head, in Department of Electronics & Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru.