Circuits and Systems, 2016, 7, 3174-3182
Published Online August 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.710270

Efficient Data Integrity Using Enhanced Secret Sharing Scheme for MANET

R. Mohandas Rengaraju[1], K. Krishnamoorthi[2]

[1]Department of Electronics and Communication Engineering, Jayaram College of Engineering, Trichy, India
[2]Department of Electrical Engineering, Sona College of Technology, Salem, India
Email: mohandasbe@gmail.com, krishrevathi25@gmail.com

Received 7 April 2016; accepted 1 May 2016; published 23 August 2016

Abstract

Mobile Ad Hoc Networks consist of nodes which are wireless and get organized based on the transmission requirement. These nodes are mobile nodes, so they communicate with each other without any fixed access point. This type of network faces several attacks because of its mobility nature. In MANET, black hole attacks may cause packet dropping or misrouting of packets during transmission from sender to receiver. This may lead to performance degradation in the network. To surmount this issue, we propose the modified secret sharing scheme to provide the data protection from unauthorized nodes, consistency of data and genuineness. In this algorithm, initially the identification of black hole attacks is achieved and followed by data protection from malicious nodes and also this scheme checks for the reality of the data. Here, we detect the misbehaviour that is dropping or misrouting using verifiable secret sharing scheme. The proposed algorithm achieves the better packet delivery ratio, misbehaviour detection efficiency, fewer packets overhead and end-to-end delay than the existing schemes. These can be viewed in the simulation results.

Keywords

MANET, Verifiable Secret Sharing, Modified Proactive Secret Sharing Scheme, End-to-End Delay, Overhead, Misbehaviour Detection Efficiency and Delivery Ratio

1. Introduction

1.1. Mobile Ad Hoc Networks (MANETs)

In recent years, MANET is not only used widespread [1] in commercial and domestic application areas but also has become the focus of intensive research. Applications of MANET's range from simple wireless home and of-

How to cite this paper: Mohandas Rengaraju, R. and Krishnamoorthi, K. (2016) Efficient Data Integrity Using Enhanced Secret Sharing Scheme for MANET. *Circuits and Systems*, **7**, 3174-3182. http://dx.doi.org/10.4236/cs.2016.710270

fice networking to sensor networks and likewise constrained tactical network environments. Data security is very important in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborated data injection attacks.

1.2. Intruders

In this type of attack, node is used to convey that this node is very near to all, which becomes cause to all nodes around it to route data packets towards it. The AODV protocol is the best to such kind of attack because of having network centric property, where each node of the network has to share their routing tables among each other.

A malicious node may use the routing protocol to advertise itself that only through that node the shortest path to the destination is available. Whenever a source node wants to send data packets to a destination node, if there is no route available in its Routing Table (RT), then it will initiate the routing discovery process. For example assume B to be a malicious node. Using the routing AODV protocol, node B claims that it has the routing to the destination node every time it gets Route Request packets, and sends the response to source node immediately. The destination node may also give a reply. If the reply from a normal destination node reaches the source node of RREQ first, everything works well; but the reply from node B could reach the source node first, if node B is nearer to the source node.

Moreover, node B does not check its routing table to send a false message to the source node and also its response time is very less when compared to the original destination node. This makes the source node thinks that the routing discovery process is completed, ignores all other reply messages, and begins to send data packets. The forged routing has been created. As a result, all the packets through node B are simply consumed or lost and it does not attain the destination node. Node B could be said to form a black hole in the network, and it is said to be the black hole attack.

2. Related Work

Amol A. Bhosle *et al.* [2] suggested the watchdog mechanism to detect the black hole nodes in a MANET. This method first find out a black hole attack in the network and then provides a new alternate path to this node. In this, the performance of original AODV and modified AODV with multiple black hole nodes is find out on the basis of throughput and packet delivery ratio. They also gave the time of flight to detect and defeat black hole attack and wormhole attack and to improve the data security in mobile ad-hoc network.

Firoz Ahmed *et al.* [3] introduced an Encrypted Verification Method (EVM) that efficiently detects a black hole attack. A detection node that receives an RREP from a trust less node sends an encrypted verification message directly to destination along the path included in the RREP for verification. The approach not only pins down the black hole nodes, but also reduces control over-head significantly. In [4], mobile agent based IDS is introduced in order to reduce the overheads. The use of distributed ID consists of multiple mobile agents which assist over a large network and to make communication with each other, or with a central server that provide advanced network monitoring, incident analysis, and instant attack data. This as a whole reduces the network bandwidth usage by moving data analysis computation to the place of the intrusion data & sustains on the heterogeneous platforms.

M. Umaparvathi and Dharmishtan K. Varughese *et al.* [5] propose a secure routing protocol, Two Tier secure Adhoc On-Demand Distance Vector (TTSAODV), which is an extension of the well known Ad hoc On-Demand Distance Vector (AODV) routing protocol that can be used to protect the route discovery mechanism against black hole attack. This paper evaluates the performance of AODV and TTSAODV protocols under black hole attack. This protocol detects and finds the secure path against single as well as collaborative black hole attacks. This protocol uses symmetric key system and verification messages to discover a safe route.

Disha *et al.* [6] demonstrated an adaptive method for detecting black and gray hole attacks in ad hoc network based on a cross layer design. In network layer, a course-based method to overhear the next hop's action is proposed. This scheme does not send out extra control packets and saves the system resources of the detecting node. In MAC layer, a collision rate reporting system is established to guess dynamic detecting threshold so as to lower the false positive rate under high network overwork. DSR protocol is preferred to test algorithm.

Sushil Kumar *et al.* [7] analyzed the performance of AODV with and without black hole (malicious node) attack under the circumstances of different parameters. Simulation results show that when a node becomes a malicious node it will effect on the AODV performance. The route discovery process in the AODV is susceptible to black hole attack and therefore, it is vital to have an efficient security functions in the protocol in order to avoid such attacks.

Ping Yi *et al.* [8] demonstrated an adaptive approach for detecting black and gray hole attacks in MANET based on a cross layer design. In network layer, a path-based method is proposed to overhear the next hop's action. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. This scheme does not send out extra control packets and saves the system resources of the detecting node.

N. Bhalaji *et al.* [9] presented a trust based routing model to deal with black hole and cooperative black hole attacks that are caused by malicious nodes. We believe that fellowship model is a requirement for the formation and efficient operation of ad hoc networks. The paper represents the first step of our research to analyze the cooperative black hole attack over the proposed scheme to analyze its performance. The next step will consist of analyzing the protocol over Grey hole and cooperative grey hole attacks.

In [10], Mehdi proposed and approach to combat the Cooperative/ Multiple Black hole attack by using negotiation with neighbors who claim to have a route to destination. The percentage of packets received through the proposed method is better than that in AODV in presence of cooperative black hole attack. In [11], Thamarai selvi presented an ant based novel approach reliability to detect anomalies. The proposed approach is decentralized, active and extensible. In order to provide better performance in the mobile architecture this work ensures security for mobile nodes. Every Mobile node is liable to attack. Such nodes were declared as malicious node. This work will provide efficient strategy to fight against threats like Black hole attack using the fitness function generated from ACO (Ant Colony Optimization).

The paper is organized as follows. Section 1 describes introduction about overview of MANETs and black hole attacks. Section 2 deals with the previous work which is related to the wormhole attacks. Section 3 is devoted for the implementation of proposed algorithm. Section 4 describes the performance evaluation and the last section concludes the work.

3. Proposed Algorithm

In the proposed algorithm Efficient Multipath Routing Tree based Energy Minimization (EMRTEM) in WSNs, there are 8 steps to achieve the minimal energy consumption through multipath routing tree. Here we added parent node, route node selection, finding multipath routing tree for message length queries and minimizing the average energy consumption. The alternative healing method is protected inside the proposed set of rules which gives the course redundancy to take away the route repair like node and link failure sessions.

3.1. Cross Layer Architecture

In our proposed scheme, a cross-layer design is proposed while the MAC layer predicts the state of the channel whether it is good or bad. This calculation depends on Rayleigh fading channel model where using the previous signal strength requirements. Once the channel is good which is determined by MAC layer, the data transmission gets started. The prediction model for the Rayleigh fading channel is cooperated with a Markovian model for IEEE 802.11 standards MAC to analyze the performance of the proposed scheme. The main reason for predicting the Rayleigh fading channel is to improve performance of the network. The mobile node at the destination end observes the power levels of each received transmission from the receiver. By using these measurements, the destination node predicts whether the channel would be in good or bad state during the next transmission phase. If it fails, then it informs the sender about the fade and stops transmission of any reply packets to the source node. The destination node may inform the source node about the forthcoming fade by setting a flag in the acknowledgment (ACK) or clear-to-send (CTS) packet that it transmits to the source node.

When the supply node receives this notification, then it right away halts the transmission, the predicted fade length is decided and schedules future transmissions accordingly. The Network Allocation Vector (NAV) at the neighbours is also updated when they overhear a CTS or ACK whose flag bit is marked. The simulation results using object oriented discrete even simulator obtained indicate the cross-layer implementation performs better than the layer implementation in terms of received signal strength, throughput, fraction of packets dropped, throughput, delivery ratio and congestion ratio.

3.2. Multipath Routing

Multipath routing has been used in several different contexts. Multipath routing technique uses the multiple alternate paths through a network which benefits fault tolerance and reliability. Traditional circuit switched telephone networks used a type of multipath routing called alternate path routing. In alternate path routing, node pair has a set of multiple paths which comprises a primary path and alternate paths. Alternate path routing was proposed in order to decrease the call blocking probability and increase overall network utilization. It is spreading of traffic from source to destination over providing many paths through network.

In alternate path routing, traffic is routed through the shortest path which is one hop. If the shortest path is engaged or unavailable due to full capacity or link failure, the traffic is routed through the alternate path which is of two hops instead of blocking the connection. When the same label traffic flows, the router dynamically splits the traffic flow into different paths based on the QoS constraints (minimum delay and maximum bandwidth).

The steps for achieving load distribution through the multipath routing are follows:

Step 1: Calculate the ℓ, a set of disjoint path from source to destination. The path is considered as a loop less path.

Step 2: Find the path χ from ℓ based on the bandwidth and (least hop) shortest path distance *i.e.*

$Bw(p_m) = Bw(p_k)$ and the distance $S_d(m) = S_d(l)$.

Step 3: If (Path failure occurs)

{

Choose the alternative backup path form the set 1 $\{P_l, P_m, \cdots, P_n\}$ with least hop distance. If the source is l and the destination n.

}

else

{

Stop the transfer of the data from source to destination.

}

Step 4:

Select the path from the maximum number of edge disjoint paths which satisfies the bandwidth and delay requirements

$$\mathrm{BW}(\mathrm{p}_l) + \mathrm{BW}(\mathrm{p}_\mathrm{m}) + \cdots + \mathrm{BW}(\mathrm{p}_\mathrm{k}) = \mathrm{BW}_\mathrm{t}(\mathrm{P}_\mathrm{T}) \tag{1}$$

$$\mathrm{DE}(\mathrm{p}_l) + \mathrm{DE}(\mathrm{p}_\mathrm{m}) + \cdots + \mathrm{DE}(\mathrm{p}_\mathrm{k}) = \mathrm{DE}_\mathrm{t}(\mathrm{P}_\mathrm{T}) \tag{2}$$

Step 5:

Establishing the multipath routing among all the mobile nodes in the network.

Step 6:

Achieving the load balancing to improve the throughput and network connectivity.

3.3. Intrusion Detection System

Step 1:

Source S wants to communicate with node D. It broadcasts the request message RREQ. RREQ includes the level of security it requires and D's id, a sequential number and P_b D $[S_{id}]$ is the Source's id encrypted by Destination's public key and Trust Active. RREQ is like this: {RREQ, seq_num, P_b D $[S_{id}]$, D_{id}, T_A}, where T_A Trust active is the time-dependent trust value. Initially node A have the trust value on node B is at time t_1; but after a certain period, node B may travel to another zone which is out of radio range of node A due to nodes mobility in MANET. At time t_2, node B happens to back in node A's radio range again. The trust value should decay during this time gap. Let ${}_AT_B(t_1)$ be the trust value of node A to node B at time t_1 and ${}_AT_B(t_2)$ be the decayed value of the same at time t_2. Then trust active is defined as follows,

$${}_AT_B(t_2) = {}_AT_B(t_1) * \mathrm{e}^{-\left({}_AT_B(n)\Delta t\right)^{2k}} \tag{3}$$

1. Node A receives RREQ. It looks up its trust list for the trust values of the neighbors. And A will encrypt if own id with proper policy and append in the message. The message which will sent by A is like this:{RREQ,

seq_num, P_b D[P_v A[A_{id}], P_bD[S_{id}], D_{id}, R_B^A} where P_v A is the private key of A, where R_B^A (Node proposal) is also used to identify the malicious behavior. Evaluating the recommendation is given by R_B^A which is node A's evaluation to node B by collecting recommendations,

$$R_B^A = \frac{\sum_{\upsilon \in \gamma} V\left|A \to C\right| * V\left|C \to B\right|}{V\left|A \to C\right|} \tag{4}$$

γ is a group of recommenders.

$V\left|A \to C\right|$ is trust vector of node A to C.

$V\left|C \to B\right|$ is trust vector of node C to B.

2. D receives RREQ. It uses its private key and the public key of the intermediate nodes to authenticate them. D checks if there are any bad nodes. If they are all trusted, D generates a number for the flow Fid , and broadcasts the following message(suppose A and B are the intermediate nodes): {RREP, Pb B[F_{id}, Pb A[F_{id}, Pb S[Pv D[F_{id}]]]]};
3. Intermediate node that receives the RREP uses its private key to decrypt the message and gets the flow id. Then it updates its route table with Fid designated to destination D;
4. S receives RREP, uses its private key to decrypt the message and D's public key to identify the destination. Afterwards, it will send message with the flow id Fid.
5. Cluster Head maintains the Trust threshold value based on trust active and node proposal to detect the attacks.
6. If any nodes below the Trust threshold value that node is encountered by an attacks.

3.4. Secret Sharing Scheme

Step 1: Let (S_1, S_2, ···, S_n) be an (t,n) sharing of the secret key S of the service with the node k having S_k.

When S_k, is defined from a finite a finite field D = Z_r and g is a primitive element in F.

Step 2: Node K (K ∈{1, 2, 3, ···, n}) which randomly generates S_k's sub shares like (S_{i1}, S_{i2}, ···, S_{in}) for (n,t) sharing.

Step 3: All subshares S_{kp} (p ∈{1, 2, 3, ···, n}) is distributed to node p through the secure link.

Step 4: When node j gets the sub shares {S_{1k}, S_{2k}, ···, S_{nk}}. It computes a new share from these sub shares and its old share with an equation.

$$S'_p = S_p + \sum_{k=1}^{n} S_{k,p} \tag{5}$$

3.5. Digital Signature Verification

Step 1: Share holder node M sends PSS_start flag to all share holder nodes.

Step 2: All Share holder nodes sends PSS_start_ack flag to the share holder node M.

Step 3: Initiated the sharing procedure.

Step 4: Node send the refresh_flag to all share holder nodes. All nodes refresh its share to send shares to other share holder nodes with digital signature and encrypted public key of destination nodes.

Step 5: Verify the digital signature trust active using trust mechanism.

Step 6: Send end flag to all share holder nodes. After receiving this end flag, send_ack flag again and send refresh_end flag to all share holder nodes.

Step 7: In detection phase, we use the concept of Virtual Sharing scheme procedure to detect any misbehaviour.

Each share holder node verify his own share by using,

$$g^{su} = \Pi_{j=0}^{k} = A_j^{\alpha_u^j} \tag{6}$$

If the share holder node does not broadcast the above information, misbehaviour will be broadcasted to all the share nodes.

Step 8: The secret key is reconstructed. If S_k holds shares (m_1, n_1) and S_p hold shares (m_2, n_2), share holder node reconstructs If $m_1 = m_2$, then the secret is n_1, otherwise the secret is n_2.

4. Performance Analysis

QualNet version 4.5 is used to simulate our proposed algorithm. QualNet is one of the best tools to analyse Mobile Ad-hoc Networks and Wireless Sensor Networks. We can easily implement the designed protocols by writing C++ Program. Visual Studio is used as an Integrated Development Environment (IDE) to develop the coding. QualNet helps to prove our theory analytically and Visual Studio is used to develop the User Interface (UI). In our simulation, 50 mobile nodes move in a 1600 meter × 1600 meter square region for 60 seconds simulation time. All nodes have the equal transmission range of 250 meters. Our simulation settings and parameters are summarized in **Table 1**.

Performance Metrics

We evaluate mainly the performance according to the following metrics.

Throughput: It is known as the number of packets delivered successfully.

End-to-end delay: It is averaged over all surviving data packets from the source to the destination.

Packet delivery ratio: The ratio of packet received to the packet sent in the network is referred as Packet Delivery Ratio. This ratio also represents the loss ratio of the routing protocol Ideally the ratio should be 1.If the ratio is less than 1,then it indicates some fault in the network design. Otherwise, if it is greater than 1 then it indicates that the sink node receives the same data packet once again. If it is so, then network resources may get wasted. Based on the number of duplicates received by the destination, appropriate action will be taken to reduce the redundancy.

Figure 1 shows the Throughput obtained for varying number of nodes from 5 to 50. From the results, we can see that EDIESSS scheme has higher delivery ratio than the SEDP and MPSS security scheme.

Figure 2 shows the End-to-End delay for varying the mobility of nodes from 5 to 50. From the results, we infer that MPSS scheme has lower delay than the SEDP scheme and EDIESSS scheme has lower than both the other methods in comparison. Minimizing the delay will directly improve the other parameters like packet delivery ratio and increased throughput.

Figure 3 shows the Packet Delivery Ratio (PDR) of network for variable number of nodes from 5 to 50 in steps 5. From the results, we can see that EDIESSS has significantly higher packet delivery ratio values than SEDP and MPSS. The higher the PDR value refers the higher network quality.

Figure 4 shows packet loss of each scheme. Lesser Packet loss causes less number of retransmissions. Thus the overall performance is inversely proportional to the packet loss. SEDP and MPSS are getting packet loss values above 16, where as proposed EDIESSS scheme lowers the packet loss and is below 16. With less number of packet loss, EDIESSS provides stable and faster communicative network architecture.

Table 1. Simulation settings and parameters.

No. of Nodes	50
Area Size	1600 × 1600
Mac	802.11
Radio Range	250 m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m^2
Package rate	5 pkt/s
Protocol	DSR

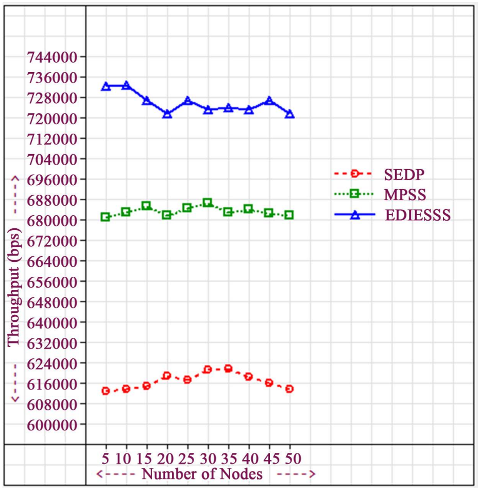

Figure 1. Throughput vs. number of nodes.

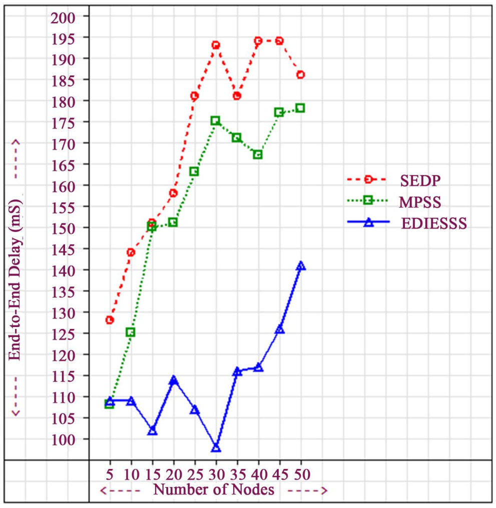

Figure 2. End-to-end delay vs. number of nodes.

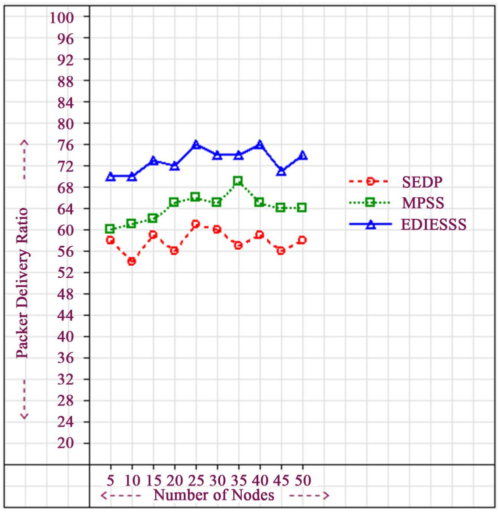

Figure 3. Packet delivery ratio vs. number of nodes.

Mobility is the ultimate freedom of MANET nodes. Higher mobility ensures stable communication while the mobile nodes are moving with higher velocity. A better security protocol must allow the nodes to move faster and with random changes in velocity as well as directions. Figure 5 shows the mobility of the procedures under observation, where EDIESSS has the highest mobility than SEDP and MPSS methods.

5. Conclusion

Wireless Ad Hoc Networks consist of wireless nodes with none centralized infrastructure. Here node may be stricken by numerous attacks. It may cause the packet losing, routing the information to some other unknown destination. In our proposed work, we focus on detection of the black hole attacks. This attack degrades the per-

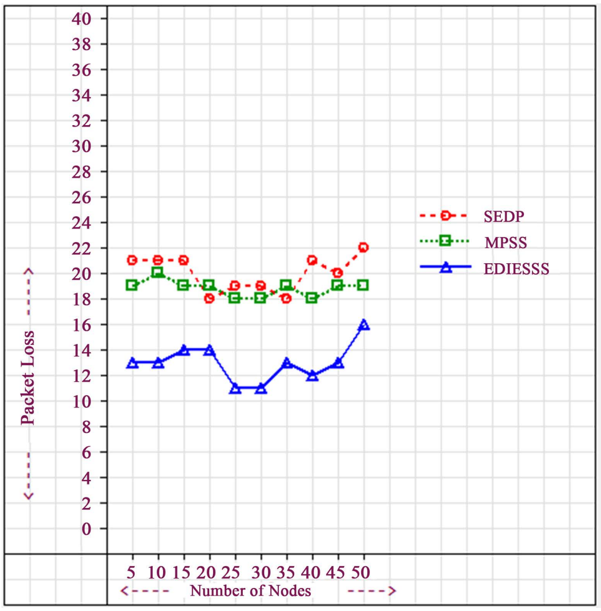

Figure 4. Packet loss vs. number of nodes.

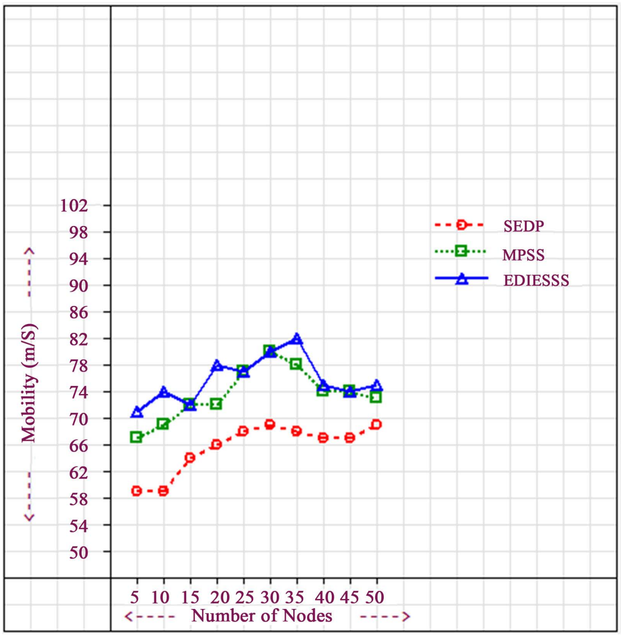

Figure 5. Mobility vs. number of nodes.

formance of the mobile ad hoc networks. So that, we advocate the modified proactive secret sharing scheme to stumble on the black hole attacks. In first segment, the black hole attacks are detected and isolated. In second segment, the proactive scheme provides the data protection from unauthorized nodes and also consistency of data and genuineness. By using the extensive simulation results, the proposed EDIESS scheme achieves better results than the existing schemes.

References

[1] Ali, M.A. and Sarwar, Y. (2011) Security Issues Regarding MANET (Mobile Ad Hoc Networks): Challenges and Solution. Thesis, 1-65.

[2] Bhosle, A.A., Thosar, T.P. and Mehatre, S. (2012) Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET. *International Journal of Computer Science, Engineering and Applications* (*IJCSEA*), **2**, 45-54. http://dx.doi.org/10.5121/ijcsea.2012.2105

[3] Ahmed, F., Yoon, S.Y. and Oh, H. (2012) An Efficient Black Hole Detection Method using an Encrypted Verification Message in Mobile Ad Hoc Networks. *International Journal of Security and Its Applications*, **6**, 179-184.

[4] Roy, D.B. and Chaki, R. (2012) BAIDS: Detection of Blackhole Attack in MANET by Specialized Mobile Agent. *International Journal of Computer Applications*, **40**, 1-6. http://dx.doi.org/10.5120/5037-7355

[5] Umaparvathi, M. and Varughese, D.K. (2012) Two Tier Secure AODV against Black Hole Attack in MANETs. *European Journal of Scientific Research*, **72**, 369-382.

[6] Kariya, D.G., Kathole, A.B. and Heda, S.R. (2012) Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method. *International Journal of Emerging Technology and Advanced Engineering*, **2**, 37-41.

[7] Chamoli, S.K., Kumar, S. and Rana, D.S. (2012) Performance of AODV against Black Hole Attacks in Mobile Ad-Hoc Networks. *International Journal of Computer Technology & Applications*, **3**, 1395-1399.

[8] Yi, P., Zhu, T., Liu, N., Wu, Y. and Li, J.H. (2012) Cross-Layer Detection for Black Hole Attack in Wireless Network. *Journal of Computational Information Systems*, **8**, 4101-4109.

[9] Bhalaji, N. and Shanmugam, A. (2011) A Trust Based Model to Mitigate Black Hole Attacks in DSR Based MANET. *European Journal of Scientific Research*, **50**, 6-15.

[10] Medadian, M. and Fardad, K. (2012) Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol. *European Journal of Scientific Research*, **69**, 91-101.

[11] Thamil Selvi, C.P. (2012) A Novel Method to Detect Black Hole Attack in MANET Using Efficient ACO Strategy for SEAD Protocol. *International Journal of Computer Applications*, **45**, 1-4.