International Journal of Soft Computing 10 (6): 408-414, 2015
ISSN: 1816-9503
© Medwell Journals, 2015

# Effective Authenticated Routing Scheme for Data Integrity in MANET

K. Vinoth Kumar and S. Bhavani
Department of ECE, Karpagam University, Coimbatore, India

**Abstract:** Mobile ad hoc networks consist of mobile nodes which are running randomly. Nodes are communicating each other without any access point. Due to mobility of nodes, network is easily affected by presence of several attacks. Particularly black hole attacks cause packet dropping, misrouting the information form source to destination. Due to that, retransmission of packets occurs unlimitedly. So, the energy consumption of nodes goes very highly. So, the performance of the network is degraded. To reduce the effect of this attack, we proposed a New Enhanced Proactive Secret Sharing Scheme (NEPSSS) to ensure the data confidentiality, data integrity and authenticity. In first phase of the proposed algorithm, the detection of packet dropping attacks is achieved using trust active and recommendation of the nodes. In second phase of the work, modified proactive scheme is used to provide the data authentication and integrity. In third phase, Energy Consumption Model is proposed to keep minimum energy consumption of nodes. By simulation results the proposed algorithm achieves the better packet delivery ratio, misbehavior detection efficiency, fewer packets overhead and low end to end delay than the existing scheme EAACK and our previous schemes like EMALRP, ELOER and TMAP.

**Key words:** MANET, enhanced proactive secret sharing scheme, end to end delay, overhead, misbehavior detection efficiency and delivery ratio

## INTRODUCTION

**Overview of MANET security:** The aims of ad hoc networks and particularly MANET have in recent years not only seen widespread use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's range from simple wireless home and office networking to sensor networks and similarly constrained tactical network environments. Security aspects play an important role 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 elaborate data injection attacks.

**Packet dropping attacks:** In this type of attack, node is used to advertise a zero metric to all destinations which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property where each node of the network has to shares their routing tables among each other.

A malicious node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. When a source node wants to send data packets to a destination node, if there has no route available in its Routing Table (RT), 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 whenever it receives RREQ packets and sends the response to source node at once. 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 need to check its RT when sending a false message; its response is more likely to reach the source node firstly. 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. Node B could be said to form a black hole in the network and we call it as the black hole attack.

## LITERATURE REVIEW

Bhosle *et al.* (2012) proposed the watchdog mechanism detect the black hole nodes in a MANET. This method first detects a black hole attack in the network and then provides a new route to this node. In this, the

**Corresponding Author:** K. Vinoth Kumar, Karpagam University, Coimbatore, India

performance of original AODV and modified AODV in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio. They also proposed the time of flight to detect and overcome black hole attack and wormhole attack and improve the data security in mobile ad hoc network.

Ahmed *et al*. (2012) introduced an Encrypted Verification Method (EVM) that effectively detects a black hole attack. A detection node that receives an RREP from a suspicious 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 overhead significantly.

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 and sustains on the heterogeneous platforms (Roy and Chaki, 2012).

Sharma and Gupta (2012) focused on black hole detection using mobile agent. The possibility of attackers arrival is reduced by means of announcing the hello messages. But, it was not focused on arrival of attackers Umaparvathi and Varughese (2012) proposes a secure routing protocol, Two Tier secure Ad hoc 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 study 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.

Kariya *et al*. (2012) demonstrated an adaptive method to 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.

Chamoli *et al*. (2012) 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 become as 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.

Yi *et al*. (2012) demonstrated the an adaptive approach to 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.

Bhalaji and Shanmugam (2011) 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 study 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.

Usha and Bose 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.

Medadian and Fardad (2012), Djahel *et al*. (2008), Ranjan *et al*. (2011) and Yadav and Kumar (2012) proposed the identification and removal of black hole attackers in MANET and its protocol AODV. The secure communication has been illustrated to justify the authenticated routing inside the network. But there was no secure secret sharing adopted to make network more secure.

Selvi (2012) 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).

Shakshuki *et al*. (2013) developed Enhanced Adaptive Acknowledgement (EAACK) for defending against malicious attacks. It does not affect network performance. In this study, researcher does not focus on reliable neighbor nodes to forward the packets. Neighbor recommendation is necessary to discover and maintain the route. In the proposed research, new certificate based intrusion detection system to achieve network reliability.

## IMPLEMENTATION OF PROPOSED ALGORITHM

New Enhanced Proactive Secret Sharing Scheme (NEPSSS) is implemented in terms of three stages like black hole attacks detection, secret sharing procedure and Energy Consumption Model to ensure the integrity of information is being carried between source and destination node.

### Detection of packet dropping attacks

**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 [$S_{i\,d}$], $D_{id}$, $T_A$}. 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:

$$ {}_AT_B\,(t_2) = {}_AT_B\,(t_1)\times e^{-({}_AT_B\,(n)\Delta t)^{2k}} \tag{1}$$

**Step 2:** 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[$A_{id}$], $P_b$D[$S_{id}$ ], $D_{id}$, $R_N{}^M$} where $P_v$ A is the private key of A. Where node proposal $R_N{}^M$ is also used to identify the malicious behavior. Evaluating the recommendation is given by $R_N{}^M$ which is node M's evaluation to node N by collecting recommendations:

$$R_N^M = \frac{\sum_{\upsilon\in\gamma} V\,|\,M \rightarrow P\,|\,{*}V\,|\,P \rightarrow N\,|}{V\,|\,M \rightarrow P\,|} \tag{2}$$

Where:

$\gamma$ = A group of recommenders  
$V|M\rightarrow P|$ = Trust vector of node M to P  
$V|M\rightarrow P|$ = Trust vector of node P to N

**Step 3:** 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 $F_{id}$ 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[$F_{id}$]]]]}.

**Step 4:** 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 $F_{id}$ designated to destination D.

**Step 5:** 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 $F_{id}$.

**Step 6:** Cluster head maintains the trust threshold value based on trust active and node proposal to detect the attacks.

**Step 7:** If any nodes below the trust threshold value that node is encountered by an attacks.

### Secret sharing procedure

**Step1:** 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:

$$S_p^{'} = S_p + \sum_{k=1}^{n} S_{k,\,p} \tag{3}$$

### Modified proactive secret sharing scheme

**Step 1:** Source node A sends his Secret sharing flag M_start to all the share holder nodes.

**Step 2:** All Share holder nodes send the M_start_ack flag to the share holder node M.

**Step 3:** Sharing procedure is initiated.

**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. The digital signature is verified using the proposed digital signature algorithm. Here, the public key F, message m, signature (p, q) is used in the input of signature verification. In output, the validation of digital signature is performed. The verification procedure is followed as:

- The signature (p, q) is the integers in between the interval [1, N-1]. If any verification fails, then the signature will be rejected. N is the order of the system
- The encryption value is calculated by:

$$e = H(m) \tag{4}$$

H denotes a hash function whose outputs have bit length not more than that of N

- The integer value is calculated as:

$$v = q^{-1} \bmod N \tag{5}$$

This integer is used to calculate the value of order of N. It is used to verify the signature of the q with respect to order N of the system:

- Convert the $u_1$ coordinate of U in to an integer $\bar{u}_1$
- Determine:

$$y = \bar{u}_1 \bmod N \tag{6}$$

- If a signature (p, q) presents on the message m which is generated by the signer (destination node signature), then $q = s^{-1}$ (e+cp) (mod N). Reshuffling as:

$$s = p^{-1}\ (e + cp) = p^{-1}e + p^{-1}cp = ve + vcp = z_1 + z_2c\ (\text{mod } N) \tag{7}$$

Thus, $X = (z_1+z_2c)$ W = sW and so y = p as required

- If y = p then the signature is accepted. Otherwise, it is rejected

**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 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 $n_2$.

First step, detecting the black hole attacks by using the node proposal and node trust threshold value is achieved. Second step, deploying secret sharing procedure to provide the integrity of the packets is achieved. Third step, implementing the energy consumption model to keep minimum energy consumption of nodes.

## PERFORMANCE ANALYSIS

Network Simulator (NS2.34) tool is used to simulate our proposed algorithm. NS2 is one of the best simulation tools available for wireless sensor networks, ad hoc networks and DTN. We can easily implement the designed protocols either by using the otcl (object oriented tool command language) coding or by writing the C++ Program. In either way, the tool helps to prove our theory analytically.

In our simulation, 100 mobile nodes move in a 1200×1200 $m^2$ region for 100 sec simulation time. All nodes have the same transmission range of 250 m. Our simulation settings and parameters are summarized in Table 1.

**Performance metrics:** We evaluate mainly the performance according to the following metrics.

**End to end delay:** The end to end delay is averaged over all surviving data packets from the sources to the destinations.

**Packet delivery ratio:** It is the ratio of packet received to packet sent successfully. This metric indicates both the loss ratio of the routing protocol and the effort required to receive data. In the ideal scenario, the ratio should be equal to 1. If the ratio falls significantly below the ideal ratio, then it could be an indication of some faults in the protocol design. However, if the ratio is higher than the ideal ratio, then it is an indication that the sink receives a data packet more than once. It is not desirable because reception of duplicate packets consumes the network's valuable resources. The relative number of duplicates received by the sink is also important because based on that number the sink can possibly take an appropriate action to reduce the redundancy.

Table 1: Simulation Settings and parameters

| Parameters | Values |
|---|---|
| No. of nodes | 100 |
| Area size | 1200×1200 |
| Mac | 802.11 |
| Radio range | 250 m |
| Simulation time | 100 sec |
| Traffic source | CBR |
| Packet size | 512 bytes |
| Mobility model | Random way point |
| Package rate | 5 pkt $sec^{-1}$ |
| Protocol | AODV |

**Throughput:** It is defined as the number of packets received successfully. We have compared our proposed scheme NEPSSS with our previous schemes EMALRP, ELOER and TMAP as well as the existing scheme EAACK. In our first experiment, we vary the no. of malicious nodes as 20, 30 up to 100.

Figure 1 show the results of detection efficiency for the nodes 20, 30, ..., 100 scenarios. Clearly, our scheme achieves more detection rate than the previous schemes. Because of cluster based routing. In this routing, link stability is maintained and malicious nodes are identified using the trust recommendation and clock based certificate determination. Therefore, the vulnerability of malicious nodes is reduced.

Figure 2 shows the results of pause time vs. communication overhead. From the results, we can see that proposed IDS achieves less overhead than previous schemes. It is because of link stability determination. Cluster head chooses only high stable link for data forwarding. So, the network delivery rate is getting increased. Packet overhead will be suppressed because of link quality and reliability of neighbor nodes.

Figure 3 shows the results of packet delivery ratio for the speed. Clearly, our system achieves more packet delivery ratio than previous intrusion detection systems. The proposed system comprises two major aspects, i.e., malicious detection and network authentication. Packet is delivered via reliable nodes through stable link. Successfully, all the packets are delivered to the destination.

Figure 4 shows the results of mobility vs end to end delay. From the results, we can see that proposed system has less delay than previous systems. End to end delay

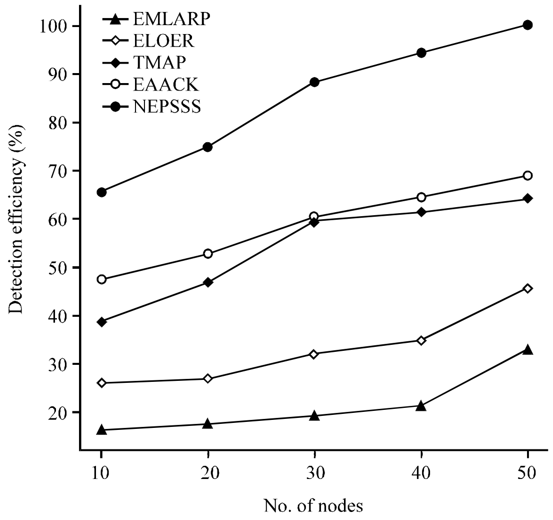

Fig. 1: No. of nodes vs. detection efficiency

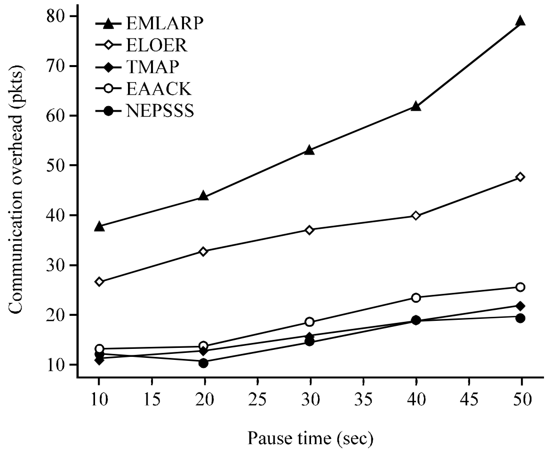

Fig. 2: Pause time vs. communication overhead

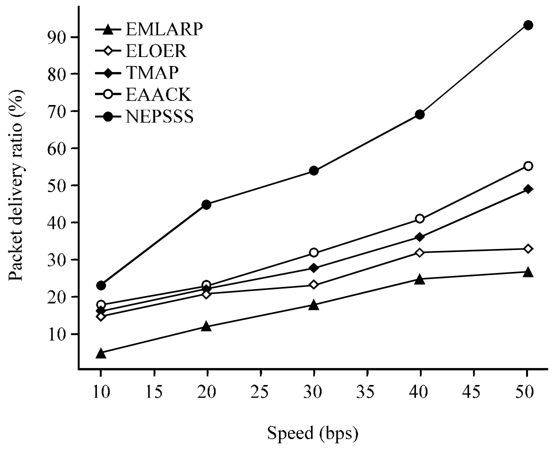

Fig. 3: Speed vs. packet delivery ratio

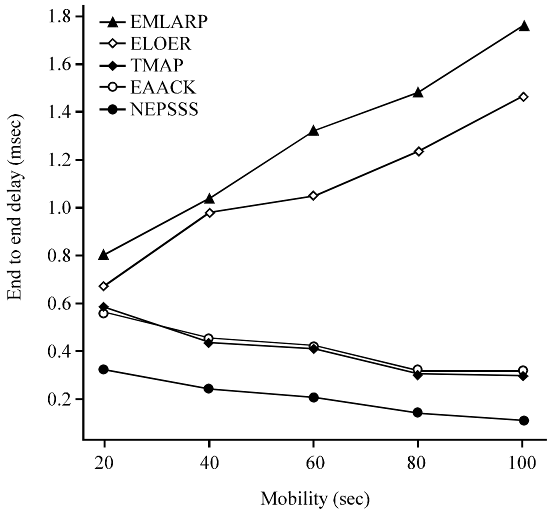

Fig. 4: Mobility vs. end to end delay

Table 2: Analysis of proposed method and existing methods in terms of different parameters

| Metrics | NEPSSS | EAACK | TMAP | ELOER | EMLARP |
|---|---|---|---|---|---|
| Detection efficiency (%) | 65-99 | 47-68 | 38-63 | 25-45 | 16-32 |
| PDR (pkts) | 23-93 | 18-55 | 16-49 | 15-33 | 5-27 |
| Network L_time (sec) | 456-987 | 256-687 | 226-667 | 100-347 | 223-440 |
| End to end delay (msec) | 0.32-0.11 | 0.562-0.315 | 0.582-0.295 | 0.678-1.47 | 0.798-1.76 |
| Overhead (pkts) | 11-19 | 12-25 | 10-21 | 26-47 | 37-78 |
| Packet integrity vs. speed | 99-92 | 76-52 | 71-48 | 64-39 | 87-65 |

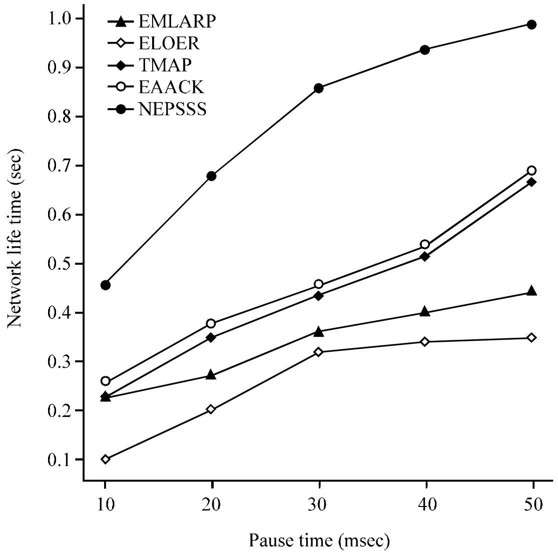

Fig. 5: Pause time vs. network lifetime

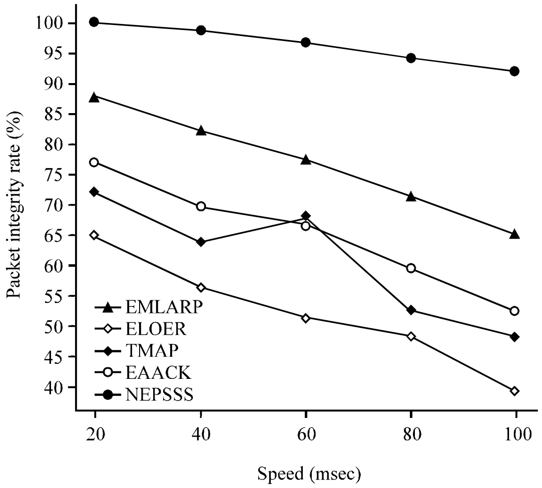

Fig. 6: Speed vs. packet integrity rate

should be kept minimum in order to satisfy QoS. The proposed system reduces delay by means of cluster based routing. Network partitioning will be reduced by integrating this routing in all networks.

Figure 5 shows the results of pause time vs. network lifetime. From the results, we can see that proposed system has more lifetime than previous systems. The proposed system increases network lifetime by adding link stability rate. Figure 6 shows the results of speed vs. packet integrity rate. From the results, we can see that proposed system has high integrity than previous systems. The proposed system increases network packets integrity based on encryption and decryption scheme performance. Table 2 presents the performance comparison of proposed and existing schemes.

## CONCLUSION

Wireless ad hoc networks consist of wireless nodes without any centralized infrastructure. Here, node may be affected by several attacks. It may cause the packet dropping, misrouting the information to another destination. In our proposed research, we focus on detection of the black hole attacks. This attack degrades the performance of the mobile ad hoc networks. So, we proposed the new enhanced proactive secret sharing scheme to detect the black hole attacks. In first phase, the black hole attacks are detected and isolated. In second phase, the authentication of data packets and data integrity is provided using the proposed secret sharing scheme. In third phase of the scheme, the energy consumption model is proposed to make minimum energy consumption of the nodes. By using the extensive simulation results, the proposed scheme achieves better results than the existing scheme EAACK and our previous schemes like EMLARP, ELOER and TMAP.

## REFERENCES

Ahmed, F., S.H. Yoon, and H. Oh, 2012. An efficient black hole detection method using an encrypted verification message in mobile ad hoc networks. Int. J. Sec. Its Appl., 6: 179-184.

Bhalaji, N. and A. Shanmugam, 2011. A trust based model to mitigate black hole attacks in DSR based MANET. Eur. J. Sci. Res., 50: 6-15.

Bhosle, A.A., T.P. Thosar and S. Mehatre, 2012. Black-hole and wormhole attack in routing protocol AODV in MANET. Int. J. Comput. Sci., Eng. Appl., 2: 45-54.

Chamoli, S.K., S. Kumar and D.S. Rana, 2012. Performance of AODV against black hole attacks in mobile ad hoc networks. Int. J. Comput. Technol. Appl., 3: 1395-1399.

Djahel, S., F. Nait-Abdesselam, Z. Zhang and A. Khokhar, 2008. Defending against packet dropping attack in vehicular ad hoc networks. Secur. Commun. Networks, 1: 245-258.

Kariya, D.G., A.B. Kathole and S.R. Heda, 2012. Detecting black and gray hole attacks in mobile ad hoc network using an adaptive method. Int. J. Emerg. Technol. Adv. Eng., 2: 37-41.

Medadian, M. and K. Fardad, 2012. Proposing a method to detect black hole attacks in AODV routing protocol. Eur. J. Sci. Res., 69: 91-101.

Ranjan, R., N. Trivedi and A. Srivastava, 2011. Mitigating of blackhole attack in MANETS.. VSRD, Int. J. Comput. Sci. Inf. Tech, 1: 53-57.

Roy, D.B. and R. Chaki, 2012. Baids: Detection of blackhole attack in MANET by specialized mobile agent. Int. J. Comput. Appl., 40: 1-6.

Selvi, T.C., 2012. A Novel method to detect black hole attack in MANET using efficient ACO strategy for SEAD protocol. Int. J. Comput. Appl., 45: 1-4.

Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. EAACK-A secure intrusion-detection system for MANETs. IEEE Trans. Ind. Electron., 60: 1089-1098.

Sharma, G. and M. Gupta, 2012. Black hole detection in MANET using AODV routing protocol. Int. J. Soft Comput. Eng.,

Umaparvathi, M. and K.D. Varughese, 2012. Two tier secure AODV against black hole attack in MANETs. Eur. J. Sci. Res., 72: 369-382.

Yadav, H. and R. Kumar, 2012. Identification and removal of black hole attack for secure communication in MANETs. Int. J. Comput. Sci. Telecommun., 3: 60-67.

Yi, P., T. Zhu, N. Liu, Y. Wu and J. Li, 2012. Cross-layer detection for blackhole attack in wireless network. J. Comput. Inf. Syst., 8: 4101-4109.