Research Journal of Applied Sciences, Engineering and Technology 6(13): 2415-2422, 2013
DOI:10.19026/rjaset.6.3716
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 13, 2013 Accepted: April 08, 2013 Published: August 05, 2013

Research Article

Secure Multipath Routing for Data Confidentiality in Mobile Ad Hoc Networks

[1]P. Sandhya and [2]Julia Punitha Malar Dhas
[1]Noorul Islam University, Kanyakumari, Tamil Nadu
[2]Department of Computer Science, Noorul Islam University, Kanyakumari, India

Abstract: In Mobile Ad Hoc Networks (MANET), the traditional way of communication performed by the nodes by choosing the geographical location causes complexity. Also the existence of malicious nodes in the transmission path may drop the data packet or influence the routing messages. In order to overcome these issues, in this study, we propose a secure multipath routing for improving data confidentiality in MANET. Initially multiple paths are established between source and destination for data transmission. In the established paths, the monitoring nodes are chosen based on the parameters such as available bandwidth and residual energy using swarm intelligence. These monitoring nodes involve in malicious node detection and informing the source of the attack. When the source wants to transmit the data to the destination, it eliminates the path with malicious nodes and bypasses the data through other alternate path. Then a secure key management technique is deployed to defend against the malicious attack. By simulation results, we show that the proposed approach enhances the data confidentiality as well as minimizes the overhead.

Keywords: ACO, authentication, bandwidth, manet, residual energy, SMRDC

INTRODUCTION

A self-configuring network consisting of mobile hosts inclusive of wireless communication devices in terms as MANET. Often, there may be random changes in the network topology as nodes are mobile. This network can either be a standalone or linked to the Internet. The nodes should be capable of transmitting traffic since the communicating nodes may perhaps be outside the transmission range. Some of the significant features that distinguish MANET from other networks are infrastructure-less, dynamic topology, low and unpredictable bandwidth and limited amount of resources, device security and physical security as well as short range connectivity. Jameela (2007) The applications of MANET are sensor networks, military operations, disaster recovery, medical support, e-commerce, vehicular traffic and accident guidance, ad-hoc communication, conferences, multi-user games, robotic pets, biological detection, mobile workspace, rescue operations, cellular network and in other vital applications (Rutvij *et al*., 2011).

The MANETs is more susceptible to security attacks rather than wired networks. Due to the facts such as restricted protection of every individual node, the uneven behavior of connectivity, deficit of certification authority, centralized monitoring or administration, security is complicated aspect to be maintained in these networks. On such a wireless network, attacks can enter from all possible directions and focus at any node. Hence each node is properly ready for facing attacks straightly or in a roundabout way. In particular, an attack from a compromised node inside the network is destructive and difficult to get identified (Sureyya and Yilmaz, 2011).

MANETs are exposed to both passive and active attacks. During active attacks, the adversary does replication, alteration and removal of swapping data. While in passive attack results in eavesdropping of data. In particular, the attacks in such a network can result in congestion, spreading wrong routing information, avoiding regular functioning of services or complete shutdown (Shanthi *et al*., 2009).

In wormhole attack, the reception of data packets at malicious node at one location followed by the tunnel the same packet to another location in the network and again re-transmission of these packets into the network is defined as wormhole attack. This attack has a possibility to get established via a wired link among two colluding attackers or through a single long-range wireless link. The technique by which the attacker utilizes the routing protocol to publicize itself that it possess shortest path to the node is said to be a black hole attack. When the malicious nodes enter the communicating path of the nodes, it has the possibility to access the packets passing through them. It further causes packet drops resulting in Denial of Service (DoS) attack. A single compromised intermediate node or group of compromised nodes works together and performs routing loop generation, packet transmission

Corresponding Author: P. Sandhya, Noorul Islam University, Kanyakumari, Tamil Nadu

over non-optimal paths and selective packet dropping resulting in routing service degradation. This kind of attack comes under Byzantine failures and it is difficult to detect such failures (Vishnu and Bhadauria, 2011).

An information disclosure, the confidential information is likely to get leaked to unauthorized nodes in the network owing to the compromised node. The confidential information includes the information concerned with network topology, geographic location of nodes or optimal routes to authorized nodes in the network. The process by which the attacker consumes resources of other existing nodes in the network is termed as resource consumption attack. The resources include battery power, bandwidth etc., which is actually available in limited quantity in the network. The attacker appears as redundant route requests, recurrent generation of beacon packets or transmission of stale packets to nodes. The illegal access made to another person's data is termed as snooping. Some of the examples of the snooping includes viewing e-mail emerging on another's computer screen or observing the content typed over other system. The complicated snoopers utilize software programs for monitoring remote activity on a computer or network devices (Rai *et al*., 2011)

In the existing system the nodes communicated by selecting a geographical location, thus creating some perimeter surrounding them and exploiting the resultant area as the destination address. Even though all the destinations within the specified area are reached using this technique, it obscures operation since the specified area may be blank. This forces the source to either enlarge the perimeter or try a different area together. The existing threshold cryptographic technique does not provide authorization and access control service. The routing performance in a cooperative manner is not explained in detail also initiates to develop an improved system.

In a MANET, the malicious node may drop the data packets or influence the routing messages. Also the malicious flooding attack causes congestion in the entire network. In order to overcome these issues, in this study we propose an effective defense technique for enhancing security in MANET.

LITERATURE REVIEW

Quansheng *et al*. (2011) have proposed a joint authentication and topology control scheme in MANET. Their technique adaptively tunes the network configuration to optimize the effective throughput and the efficiency of authentication protocols with cooperative communications. They employed a discrete stochastic approximation approach in the proposed scheme to handle the imperfect channel knowledge and the dynamically changing topology.

Ayyaswamy and Srinivasan (2010) proposed an umpiring system to offer security for routing and data forwarding operations in mobile ad hoc networks. This umpiring system has three models that include single umpiring system, double umpiring system and triple umpiring system. In their system, every node in the path performs packet forwarding and umpiring from source to destination. Instead of applying cryptographic technique, they utilize flagging technique. Through this method, when the umpiring node detects any misbehavior, those guilty nodes are flagged.

Murugan and Shanmugam (2009) have proposed a key distribution and authentication system for mobile ad hoc network. Their approach combines identity-based and threshold cryptography for offering flexibility and efficient key distribution. Further the ability for an arbitrary pair of devices to exchange a key in a secure fashion is guaranteed. This process is irrespective to the MANETs size which is varied due to the nodes mobility and also offers end-to-end authentication.

Mashud *et al*. (2011) have proposed an enhanced DSR protocol for routing packets between hosts in an ad hoc network. Their protocol uses acknowledgement and trust value calculation technique in addition with dynamic source routing which adapts quickly to routing changes when host movement is frequent. Moreover the technique ensures security against spoofing and route modification attacks. Since their protocol requires route request message to be sent twice, there is degradation in the time required for a message to reach destination. This causes tradeoff between security and speed of message transmission.

Sarwarul Islam Rizvi *et al*. (2010) have proposed a security scheme for protecting mobile agents and agent server in ad hoc network using threshold cryptography technique. Their technique offers solution to the problems concerned with central certificate authority and trusted third party in PKI by distributing trust among several network nodes. It also offers security services that include confidentiality, integrity and authenticity. The method that offers authorization and access control service is not provided in this approach.

Karim and Tsudik (2011) have proposed an on-demand location based anonymous MANET routing protocol (PRISM). Their protocol relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. It utilizes group signature schemes and location based forwarding mechanism. As this scheme discloses less of the topology, it is more privacy friendly.

PROPOSED SECURE MULTIPATH ROUTING TECHNIQUE

In this study, we propose a secure multipath routing for data confidentiality in MANET. Initially, multiple paths are established between source and destination for data transmission. In the established paths, the nodes with maximum available bandwidth

and residual energy are chosen as monitoring nodes using swarm intelligence. These monitoring nodes help in detecting the malicious nodes and it informs the source in case of detecting an attack. When the source wants to transmit the data to the destination, it eliminates the path with malicious nodes and bypasses the data through other alternate path. Then a secure key management technique is deployed that offers data privacy not only at intermediate malicious nodes but also at destination.

The link capacity is measured as the sum of the CR_{ij} and AB_i which is expressed as follows:

$$LC_i = CR_{ij}+AB_i \quad (1)$$

where, AB represents the available bandwidth, LC_i be the link capacity related to one-hop neighbor I and CR be the collective rates assigned to all ingress and egress flows.

Following the measurement of link capacity, the available bandwidth is defined using Eq. (2):

$$AB_j \underset{=}{\Delta} \max \{0, LC_j - CR^{ij}\} \quad (2)$$

The Residual Energy (RE) is computed by every node in the network by monitoring its energy consumption for transmission and reception process every t seconds:

$$E_{tx}(z, d) = (E_d*z) + (E_{tx}*z*d^2) \quad (3)$$

where,

E_d = The energy dissipated during transmission and reception
d = The distance between the nodes
E_{tx} = The energy consumed by the node during packet transmission
E_{rx} = The energy consumed by the node during packet reception

The energy consumed to transmit a data packet of size z units to distance d is computed using following Eq. (3)

The energy consumed to receive a data packet of size z units is computed using following Eq. (4):

$$E_{rx}(z) = E_d*z \quad (4)$$

The total energy consumed while transmitting the data packet is computed using Eq. (6):

$$E_t = E_{tx} + E_{rx} \quad (5)$$

After the transmission and reception of a packet of z units, the residual energy of the node I is computed as follows:

Table 1: The format of route request message

Format of route request message			
Source ID	Sequence number	Destination ID	Previous hop node ID

$$RE_i = RE_{ini}-E_t \quad (6)$$

where, RE_{ini} is the Initial energy of the node (Dilip Kumar and Vijaya Kumar, 2009).

Our proposed technique mainly concentrates on improving the data confidentiality in the network. It involves three phases namely.

- Multipath route discovery
- Attack detection
- Security mechanism

Multipath route discovery: The steps involved in the multipath route discovery are as follows:

- When S wants to transmit DP to D, it initially verifies its RR for the availability of appropriate route to D
- If RR(S) = empty then S $\xrightarrow{R_{rq}}$ N_i end if

The Step 2 implies that when the route reserve of the source does not contain any route to destination, the route discovery process is initiated by the source through a broadcasting of route request message.
The format of R_{rq} message is shown in Table 1.

- N_i upon receiving R_{rq} updates its routing table with the source ID, sequence number, destination ID and previous hop node ID and it examines its destination ID

If $N_i \neq D$ then N_i rebroadcasts R_{rq} to its neighboring nodes.

else $N_i \xrightarrow{R_{rp}}$ S end if

If N_i corresponds to the intended D, it sends R_{rp} to S. Otherwise it re-broadcasts the R_{rq} to its neighbors. This process is repeated till R_{rq} reaches D.

- If N_i receives two R_{rq} with similar request ID, then the first request packet gives priority and other packet is discarded
- When D receives R_{rq}, it unicasts R_{rp} packet for each received R_{rq} in the reverse path towards S
- D $\xrightarrow{R_{rp}}$ S
- Each N_i that receives R_{rp} updates its routing table and then unicasts this R_{rp} in the reverse-path using the Euler-stored previous-hop node information
- The step v is repeated till R_{rp} reaches S
- S then utilizes the multiple routes chosen from the information received from R_{rp} for data transmission

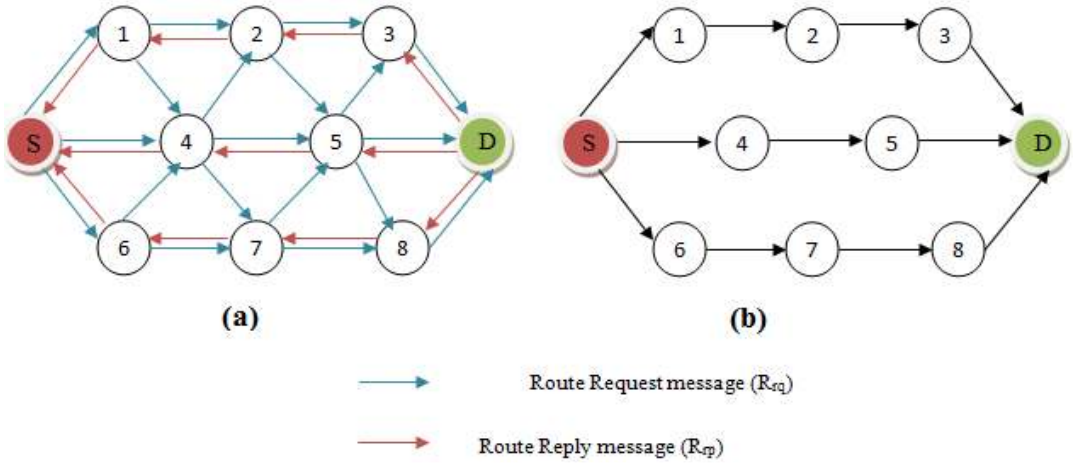


Fig. 1: (a) Route Discovery Mechanism; (b) Multipath Route Establishment

where,

S, D = The source and destination
R_{rq} = Route request message
R_{rp} = The route reply message
DP = The data packet
RR = The route reserve where the nodes stores its routing information
N_i = The intermediate nodes

(where i = 1, 2, 3 ,…,n) and ACK represent the acknowledgement.

Figure 1 demonstrates the route discovery mechanism. When S wants to transmit the data packet, it initially broadcasts the route request message to its neighboring nodes N_1, N_4 and N_6. These nodes upon receiving a request to verify whether they are intended destination. As they are not intended destination, N_1, N_4 and N_6 rebroadcasts the request to its neighbors {N_2, N_4}, {N_2, N_5 and N_7} and {N_4, N_7} respectively. As N_2 receives the request from N_1 as well as N_4, it chooses the request received first and discards the other request. Every intermediate node performs this similar action till the request packet reaches D. When D receives each route request packet unicasts reply packet in the reverse path towards S. S then chooses the multipath say {S-N_1-N_2-N_3-D}, {S-N_4-N_5-D} and {S-N_6-N_7-N_8-D}obtained from information of reply packets for data transmission.

Phase-2: Detection of malicious nodes: The detection of malicious nodes involves two steps. The first step involves the selection of Monitoring Nodes (MoN) based on the parameters such as residual energy and bandwidth using swarm intelligence based ant colony optimization. The second step involves the detection of malicious nodes utilizing the monitoring nodes.

Step 1 Monitoring node selection: Let FA be the forward ant agent, BA be the backward ant agent FA is launched by S and it visits each N_i along each path with the mobility which is estimated based on the probabilistic decision rule (shown in Eq.7):

$$Pv(Ni,S)=\begin{cases}\dfrac{[p_1(N_i,S)]^{\alpha}.[p_2(N_i,S)]^{\beta}}{\sum_{N_i\in N_{rx}}[p_1(N_i,S)]^{\alpha}.[p_2(N_i,S)]^{\beta}}, \\ 0, otherwise\end{cases}$$

$$\text{if } v \notin E(N_i) \quad (7)$$

Table 2: The format of pheromone table

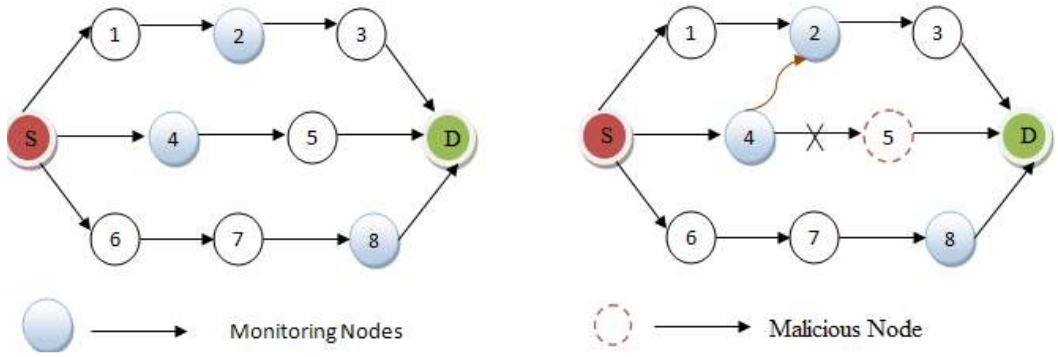
Format of pheromone table			
Source node ID	Destination ID	Available bandwidth (AB)	Residual energy (RE)

where,

$p_2(N_i, S_o)$ = The heuristic value related to bandwidth
N_{rx} = The receiver node
$E(N_i)$ = The routing table for N_i
α, β = The parameters that control the relative weight of the pheromone and heuristic value, respectively

FA upon reaching each N_i gathers the nodes status and stores in its pheromone table (Shown in Table 2).

FA upon reaching D transfers the collected status of all the nodes into BA which is generated in D. BA traverses the similar path travelled by the FA but in the opposite direction. It then updates the pheromone table with the available bandwidth and residual energy of the corresponding N_i. When BA reaches S, it transfers the status of all the nodes. S chooses the nodes with maximum available bandwidth and residual energy as monitoring nodes. Figure 2(a) illustrates the selection of monitoring nodes. N_2, N_4 and N_8 with maximum available bandwidth and residual energy are chosen as MoN.



(a) (b)

Fig. 2: (a) Monitoring node detection; (b) Malicious node detection

Step 2 Malicious node detection: The selected MoNs continuously monitors its adjacent nodes within the transmission range and gathers the nodes status:

If ($AB_i < AB_{th}$) and ($RE_i < RE_{th}$) then
The node is marked as malicious

$$MoN \xrightarrow{warning\_message} S$$

end if

When S wants to transmit the data packet to D, it discards the path with malicious nodes and transmits the data packet through the alternate available paths in the direction of D. This process is illustrated in Fig. 2(b).

The MoN (N_4) detects N_5 to be malicious node and sends the warning message to S. So while transmitting data packets discards the path {S - N_4- N_5-D} and utilizes the alternate path {S - N_4- N_2-N_3- D}.

Phase-3 Security mechanism: When S receives the warning message, it initiates a key management scheme for securing the data transmission in the network. S chooses a secret number (f), a large co-prime (u, v) and generates a common key (K_S) which is shown below:

$$K_S = u^f \bmod v \quad (8)$$

Similarly, D chooses a secret number (g) and generates a common key (K_D) which is shown below:

$$K_D = u^g \bmod v \quad (9)$$

Both S and D possess common shared key which is generated as follows:

$$K_{sh} = u^{fg} \bmod v$$

S in prior to transmitting the data, splits the data into n packets and encrypts it with K_S, source and destination IDs. Subsequently, the intermediate node IDs are attached to the data packets without encryption. This permits N_i to extract the source and destination IDs. Each time N_i receives a DP, it simply forwards this packet to the next hop node. Without the need of knowing the source and destination address, all the packets will arrive to D. When all the n packets are received, D uses K_{sh} to extract the source and destination address in each packet and compares it with its destination address.

If packet is for the node then
It decrypts it using K_{sh}. else
The packet is dropped and also cannot try to decrypt the packet.
end if

This technique offers data privacy not only at intermediate malicious nodes but also at destination.

Table 3: Simulation parameters

No. of nodes	25, 50, 75 and 100
Area	750×750
MAC	802.11
Radio range	250 m
Simulation time	50 sec
Traffic source	CBR
Routing protocol	SMRDC
Packet size	512 Bytes
Mobility model	Random way point
Speed	5 m/s
Pause time	1 sec
No. of attackers	1, 2, 3, 4 and 5.
Initial energy	10.1 J
Initial sending power	0.660
Initial receiving power	0.395

EXPERIMENTAL RESULTS

Simulation parameters: We use NS2 [http:///www.isi.edu/nsnam/ns] to simulate our proposed Secure Multipath Routing for Data Confidentiality (SMRDC) protocol. In this simulation, the channel capacity of mobile hosts is set to the value of 2 Mbps. We use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It

has the functionality to notify the network layer about link breakage. In our simulation, the number of nodes is varied as 25, 50, 75 and 100. The mobile nodes move in a 750 m×750 m^2 region for 50 sec simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 m. In our simulation, the number of attackers varied as 1,2,3,4 and 5. Random Way Point mobility model is used. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in Table 3.

Performance metrics: We evaluate performance of the new protocol mainly according to the following

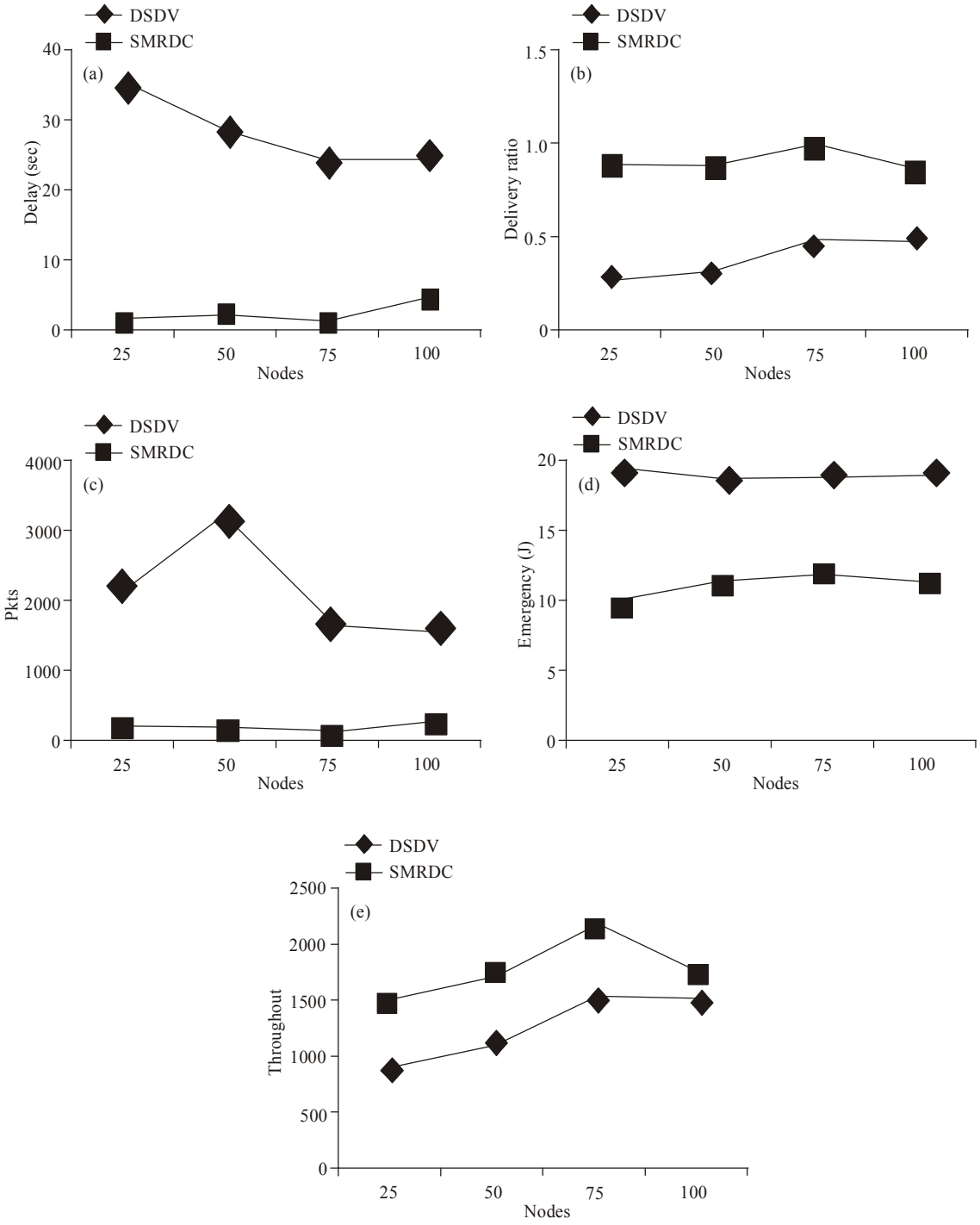


Fig. 3: (a) Nodes Vs Delay, (b) Nodes VS Delivery Ratio, (c) Nodes Vs Drop, (d) Nodes Vs Energy, (e) Nodes Vs Throughput

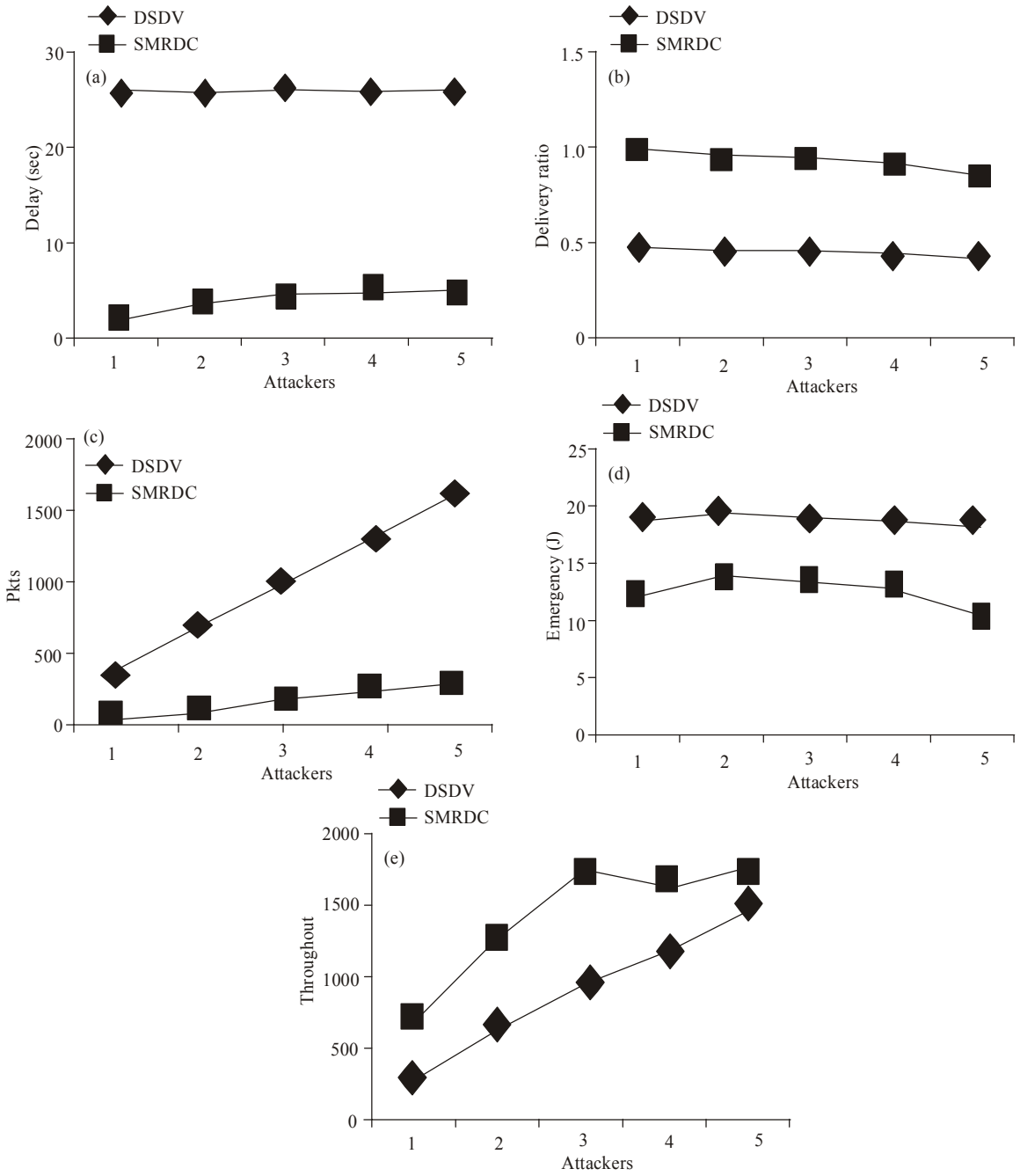


Fig. 4: (a) Nodes Vs Delay, (b) Nodes VS Delivery Ratio, (c) Nodes Vs Drop, (d) Nodes Vs Energy, (e) Nodes Vs Throughput

parameters. We compare the DSDV routing protocol with our proposed SMRDC protocol.

Average packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

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

Energy consumption: It is the amount of energy consumed by nodes during the data transmission.

Throughput: It is the number of packets successfully received by the receiver.

Packet drop: It is the number of packets dropped during the data transmission

Results and analysis: In our proposed system the simulation analysis are carry out by two basic creteria

Based on Nodes and based on delivery. Initially we vary the number of nodes as 25, 50, 75 and 100.

Based on node: In Fig. 3a, we can see that the average end-to-end delay of our proposed SMRDC protocol is less than the existing DSDV protocol. In Fig 3(b), we can see that the delivery ratio of our proposed SMRDC is higher than the existing DSDV protocol. In Fig. 3c, we can see that the packet drop of our proposed SMRDC is less than the existing DSDV protocol. In Fig. 3d, we can see that the energy consumption of our proposed SMRDC is less than the existing DSDV protocol. In Fig. 3e, we can see that the throughput of our proposed SMRDC is higher than the existing DSDV protocol.

Based on attackers: In our second experiment we vary the number of attackers as 1, 2, 3, 4 and 5.

In Fig. 4a, we can see that the average end-to-end delay of our proposed SMRDC protocol is less than the existing DSDV protocol. In Fig. 4b, we can see that the delivery ratio of our proposed SMRDC is higher than the existing DSDV protocol. In Fig. 4c, we can see that the packet drop of our proposed SMRDC is less than the existing DSDV protocol. In Fig. 4d, we can see that the energy consumption of our proposed SMRDC is less than the existing DSDV protocol. In Fig. 4a, we can see that the throughput of our proposed SMRDC is higher than the existing DSDV protocol.

CONCLUSION

In this study, we have proposed a secure multipath routing for improving data confidentiality in MANET. Initially multiple paths are established among source and destination for data transmission. In the established paths, the monitoring nodes are chosen based on the parameters such as available bandwidth and residual energy using swarm intelligence based ant colony optimization. These monitoring nodes involve in malicious nodes detection and informing the source on attack. When the source wants to transmit the data to the destination, it eliminates the path with malicious nodes and bypasses the data through other alternate path. Then a secure key management technique is deployed to defend against the malicious attack. This technique offers data privacy not only at intermediate malicious nodes but also at destination. By simulation results, we have shown that the proposed approach enhances the data confidentiality as well as minimizes the overhead.

REFERENCES

Ayyaswamy, K. and R. Srinivasan, 2010. A system of umpires for security of wireless mobile ad hoc network. Int. Arab J. E-Technol., 1(4).

Dilip Kumar, S.M. and B.P. Vijaya Kumar, 2009. EAAC: Energy-Aware Admission Control Scheme for ad hoc networks. Int. J. Comput. Int., 5(2): 125.

Jameela, A.J., 2007. Routing security in open/dynamic mobile ad hoc networks. Int. Arab J. Inf. Technol., 4(1).

Karim, E.D. and G. Tsudik, 2011. Privacy-preserving location-based on-demand routing in MANETs. IEEE J. Sel. Area. Comm., 29(10).

Mashud, R., A. Khan and S.S. Rahman, 2011. Routing security in mobile ad hoc networks: An extension of DSR. J. Emerging Trends Eng. Appl. Sci., 2(1): 155-159.

Murugan, R. and A. Shanmugam, 2009. Key distribution system for MANET with minimum prior trust relationship. Int. J. Recent Trends Eng., 1(2).

Quansheng, G., F.R. Yu, S. Jiang and V.C.M. Leung, 2011. A joint design for topology and security in manets with cooperative communications. IEEE International Conference on Communications (ICC), 5-9 June, Guangzhou, China, pp: 1-6.

Rai, A.K., R.R. Tewari and S.K. Upadhyay, 2011. Different types of attacks on integrated MANET-internet communication. Int. J. Comput. Sci. Security, 4(3): 245-274.

Rutvij, J., K. Dangarwala and N. Bhanot, 2011. Security and service discovery issues in mobile ad-hoc networks. Int. J. Networ., 1(1): 01-03.

Sarwarul Islam Rizvi, S.M., Z. Sultana, B. Sun and M. Washiqul Islam, 2010. Security of mobile agent in ad hoc network using threshold cryptography. World Acad. Sci. Eng. Technol., 70: 424.

Shanthi, N., L. Ganesan and K. Ramar, 2009. Study of different attacks on multicast mobile ad hoc networks. J. Theor. Appl. Infor. Technol., 6(4): 45.

Sureyya, M. and G. Yilmaz, 2011. A distributed cooperative trust based intrusion detection framework for MANETs. The 7th International Conference on Networking and Services (ICNS), pp: 292-298.

Vishnu, K.S. and S.S. Bhadauria, 2011. Agent based bandwidth reservation routing technique in mobile ad hoc networks. Int. J. Adv. Comput. Sci. Appl., 2(12).