Wireless Netw (2017) 23:345–354
DOI 10.1007/s11276-015-1161-3

Secure way routing protocol for mobile ad hoc network

Jarupula Rajeshwar[1] · **Gugulotu Narsimha**[2]

Published online: 21 December 2015

Abstract Mobile adhoc network is dynamic in nature and it operates completely in an infrastructure-less environment. It discovers the way routes dynamically to reach the destination. Securing a dynamic way route, which is not known before establishing communication, is always a challenge in the mobile ad hoc network. Most of the existing secure routing protocols target to evade specific type of attacks or malicious behaviour of the nodes or networks. We propose a novel secure way routing protocol for securing the dynamic way routes in MANET. It provides a unique session key for each route to secure the data communication. Moreover, it authenticates the data packets using asymmetric cryptography and secures the routing field message using two-way asymmetric cryptography. The proposal is implemented and tested for assessing the protocol's performance. We have also compared the protocol with the other secure routing protocols for evaluating its performance.

Keywords Secure routing · SWR · MANET · AODV · Cryptography

1 Introduction

Mobile ad hoc networks offer unique benefits and versatility in wireless environments as well as its applications [1–4]. It does not require any fixed infrastructure, which includes base stations and prerequisites as well [5]. But, at the same time, it is more vulnerable than the traditional wired network due to its dynamic nature and inadequate protection system [6, 7]. The vulnerability has increased, when the technological advancements has undergone the transition from a single-hop network to a multi-hop network [8]. It has also been considered as one of the primary challenges due to the network's inherent design [9]. It is intrinsically fault-resilient as the boundary of operation is not limited with respect to topology, delay constraints [10–12] and the internet usage [13–17]. It is very challenging to secure ad hoc routing because of the difficulty in maintaining any centralized policy or scheme of the traditional network [18]. Many adhoc routing protocols have been proposed in the past [19–23]. They have supported dynamic infrastructure that are unpredictable and instantly changing [24]. However, very few proposals have targeted the security requirements. [25] Most of the proposals have been found to inherently trust all the participants in the network, thus making it highly vulnerable [26, 27].

In contrast, the security threats can be from multiple sources such as, external attackers [14], intruders and greedy nodes of the network [28]. The design of routing protocol was earlier supported using an ideal loss-free channel model. Yet, the external factors such as, environmental noise, fading and collisions often degrades the quality of the links [29–31]. Besides the above- mentioned difficulties, the resources in MANET also serve as the major constraints. The reason is that they create challenges, while deploying the security processes. They have become sensitive, since the state-of-the-art routing mechanisms emphasize green communications and energy efficiency [32]. Such protocols have insisted spatial re-usability and hence, achieve high end-to-end throughput [33]. AODV [34] and DSR [35] are the two widely known reactive

✉ Jarupula Rajeshwar
rajeshwarj.2013@gmail.com

[1] Department of Computer Science and Engineering, JNTUH College of Engineering, JNTUH, Kukatpally, Hyderabad, Telangana 500 085, India

[2] Department of Information Technology, JNTUH College of Engineering, Kondagattu, Jagityal, Karim Nagar, Telangana, India

routing protocols that are very efficient in routing, but both are subjected to variety of attacks.

In this paper, we present a Secure Way Routing (SWR) protocol through modifying the conventional AODV routing protocol to address the security challenges in MANET. In SWR, each route to the destination is secure with a unique session key. Using unique session key for each route is a novel contribution of this work. It provides a security model, in which the messages involved in communication are secured using symmetric cryptography. Additionally, the way routing is authenticated with asymmetric cryptography. It secures data routing using a unique secret key that is generated using the session key of the route. This will provide a clear performance advantage such as, high throughput, low end-to-end delay and limited routing overhead. To evaluate the proposal, we have compared SWR with the other protocols like, AODV, Authenticated Routing for Ad hoc Networks (ARAN) [36], Secure AODV(S-AODV) [37] and Stable Route AODV (SR-AODV) [38].

The rest of the paper is organized as sections. Section 2 describes about the related works, which provide an overview of few routing protocols such as, AODV, ARAN, SAODV and SR-AODV. In Sect. 3, we explain the secure way routing protocol mechanism in detail. Section 4 gives the discussion on the experimental results and the corresponding evaluations. Section 5 concludes the paper.

2 Related works

A number of adhoc routing protocols have been proposed in [39–42], which have security vulnerabilities due to the wide as well as the open communication environment. These vulnerabilities are now common in mobile adhoc routing protocols also. This paper investigates about the ways to overcome these vulnerability issues, while exploring the existing securing protocols and schemes of AODV, ARAN, S-AODV and SR-AODV.

2.1 Adhoc on-demand distance vector (AODV) routing protocol [34]

AODV is a reactive routing protocol for mobile adhoc network, which constructs the route on demand. It offers low network overhead and uses sequence numbers to ensure prevention from routing loop. Basically, it uses three types of messages to perform communication and maintenance and they are: RREQ, RREP and RRER. It uses table driven routing mechanism for routing the data packets to the destination nodes. Securing the routing message is the main concern in AODV routing. It requires an authentication for securing the messages of the sender as well as the receiver. During route request broadcast, each node checks the originator's sequence number in the RREQ message against the stored information in the routing table. If a node finds a new request, it updates its routing table. For route reply, it checks the destination node's sequence number, instead of checking the originator's sequence number and keeps the routing information updated. Any vulnerability attacks will result in routing loops. Besides routing message modification, spoofing and many other attacks are also the serious issues that are relative to the AODV protocol [34].

2.2 Authenticated routing for adhoc networks (ARAN)

Sazgiri et al. [43] have proposed ARAN for securing the routing mechanism from the unauthorized participation, route modification, spoofing, message modification etc. ARAN is based on an on-demand routing protocol, which extends the features of the AODV protocol. It provides route message integrity and non-repudiation as the minimal part of the security policy in MANET.

ARAN proposes security process in three stages, namely, preliminary certificate process, end-to-end authentication and secure optimal shortest path. It uses trusted certificate server *TC* and public key cryptography to implement the three stages. Each node must acquire certificate form *TC* before joining the network. The authentication scheme of the ARAN provides protection against route or message modification, fabrication and impersonation. A launch of denial-of-service attack using a group of malicious nodes through simply broadcasting a larger number of route denial packets exhausts the computational resource to verify the signature and to generate the new ones. This drawback of ARAN utilizes extra bandwidth for transmitting the certificate and creates more routing overhead. ARAN also fail to detect the internal attacks as all the nodes in the network trust each other and cooperate to provide a stable communication [44, 45]. Hence, in case of malicious node presence, it might create huge disturbances.

2.3 Secure AODV (SAODV)

Zapata et al. [37] have proposed Secure–AODV to secure the AODV routing protocol due to numerous security vulnerabilities in the protocol. The reason is that it allows a malicious intermediate node for spoofing its identity illegally, modifying the hop count on route request messages and also to fabricate the route error messages. SAODV is an extension of the AODV protocol, which is based on the public key cryptography to provide routing security. It uses RREQ, RREP and RERR as the routing messages that are digitally signed, in order to secure and guarantee the

integrity and authenticity. Every time, a node that generates a routing message signs in with its private key and the nodes that receive this message will verify the signature using the sender's public key to authenticate. The hop count cannot be signed with the sender because it must be incremented at every hop. Therefore, in order to protect it, a mechanism based on hash chains is used. It generates bigger messages due to heavy weight symmetric cryptography that is used for digital signature. Every time, the messages received in the intermediate nodes must verify the signature for authentication. It increases the burden, when the double signature mechanism is used for generating and verifying a single message.

2.4 Secure routing with the AODV (SR-AODV) protocol

A. Pirzada et al. [38] have proposed Secure Routing with AODV (SRAODV) protocol for securing the routing. It works based on the mechanism of key exchange and data protection. It suggests node to node symmetric encryption for all the information in RREQ, RREP and RERR. It uses a group session key mechanism to negotiate with the neighborhood nodes. This protocol design requires each node to maintain additional information about the associated group members and the session key. This makes it less efficient, when the number of nodes in the network increases and it may also interrupt the normal routing for compromising the modification in hop count or destination sequence.

3 Secure way routing (SWR) protocol

In adhoc routing protocol, the nodes exchange information to their neighborhood and constructs a virtual network for routing the data packets to their desired destination. Such information can be easily targeted by any malicious adversary, who intentionally wants to disrupt the functionality of the network. The attackers generally inject erroneous routing information externally to repeat the previous routing messages or to modify the valid routing information and eventually, bring the network down. Sometimes, due to internal attacks, severe damages are produced as these nodes are not up to their initial commitments. Such nodes also can send erroneous information to modify the local view of the network. Usually, it is very difficult to identify the internal attacker because they already have some sort of credentials that everybody believes.

SWR targets both the external as well as the internal attacks that exist in the network due to malicious nodes. It identifies these attacks based on the three security mechanisms, namely, Certificate Acquisition, Secure Route Discovery and Secure Data Routing. It uses Certificate Authority (CA) certificate to identify the internal attackers and uses both symmetric as well as asymmetric cryptography for getting secured from the external attackers. To prevent the routing information from being forged or tampered, we use CA certificate for encrypting the messages.

3.1 Acquisition of certificate

Establishing security association between the mobile nodes is the most difficult part in the ad hoc network. The difficulty is due to the nature of the mobile ad hoc networks, where the predefined architecture for the security one cannot be used. Most works that are related to security association and key distributions have not been addressed well in most of the previous secure routing protocols. One simplest solution is described in [46] for the existence of security association between the source and the destination nodes. A group key exchange is described in [47], which is based on a strong sharing key. But, this approach required static group nodes and in dynamic networks, where the nodes join and leave very frequently, the group key should be updated using a process for all the nodes.

In [48, 49], another security association process among the nodes has been described. Here, any node in the network can issue certificate for the new nodes and uses asymmetric cryptography. This is a strong approach because it does not have any single point failure in the network. But, it can still have vulnerability attacks during the authentication of a new node and issue a certificate as risky, if malicious nodes are already present in the network. In SWR protocol, in order to have an initial security association among the nodes, we distribute the certificates. But, these certificates are obtained from a trusted certified authority (CA) and it has to be loaded to each node I prior to joining the network. This will be an offline process, where each node has to provide their identity to CA to obtain their certificate.

In this approach, any node that tries to possess an invalid certificate illegally can be identified and isolated easily. The certificate issued from the *CA* for a node *N* will have a CA public key as CA_{pub_key}, node address as N_{add}, public key as N_{pub_key} and private key as N_{pvt_key}. The certificate is represented as:

$$C_N = Enc_{CA_{pkey}}\left(N_{add}, N_{pub\_key}, N_{pvt\_key}, CA_{pub\_key}\right). \quad (1)$$

We assume that all the valid nodes in the network would obtain this certificate before joining the network. This process of acquiring the certificate provides basic identification to the node and prevents it from internal malicious attacks.

3.2 Secure route discovery mechanism

Our protocol modifies the AODV routing protocol to provide the secure routing mechanism as given in Fig. 1. AODV is a reactive protocol, which accomplishes its communication through the processes like, route discovery, data routing and route maintenance.

Whenever a source node N wants to communicate with a destination node D in the network, it initiates the route discovery process through sending an RREQ message. To make the discovery process secure, the SWR creates a session key using Diffie-Hellman algorithm as S_{key} and then, creates the encrypted message signature using SHA1 algorithm as S_{m_sign} and the encrypted message cipher using CA_{pub_key} as E_{msg}. Before broadcasting, the message is encrypted again using CA_{pub_key} as shown in equation-2. The idea of encrypting the message twice makes it highly secure from the attackers, who are both internal and external. The broadcast message with timestamp T can be represented as:

$$M_{rreq} = Enc_{CA_{pub\_key}}\left[S_{m\_sign}, E_{msg}, S_{key}, D_{add}, T\right] \quad (2)$$

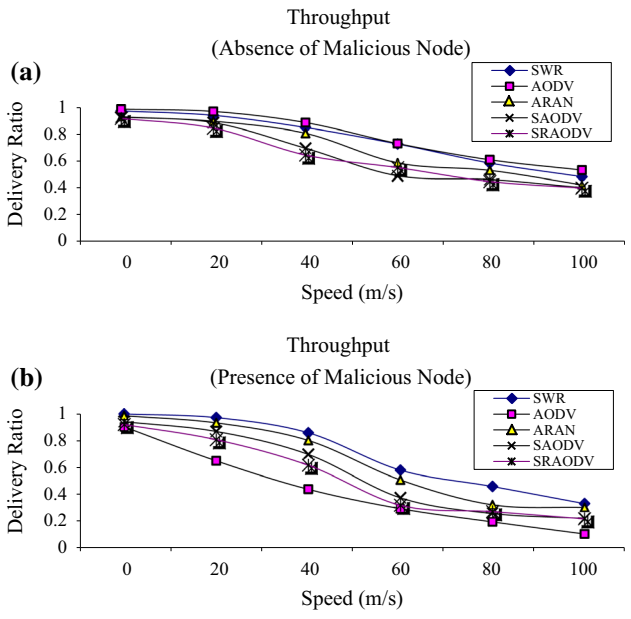

Fig. 1 Throughput performance of the proposed protocol, **a** with no malicious nodes and **b** 40 % malicious nodes

Therefore, the SWR protocol is capable of determining the secure route through making a comparison among the security parameters, while performing the route discovery of each individual node. The mechanism involved in the route discovery process is described below in Algorithm 1.

Algorithm 1: SWR Secure Route Discovery Mechanism

Source Node N init RREQ -> Init_Request(N_{rreq})

Method1: *Init_Request(Node$_{rreq}$)*

N Create Session Key using DH Algorithm → S_{SKey}

N *Encrypt(Msg)* using SHA1 Algorithm → S_{m_sign}

N *Encrypt(Msg)* using CA_{pub_key} → E_{msg}.

N *Encrypt([S_{m_sign} , E_{msg} , S_{SKey} , D_{add}, T])* using CA_{pub_key} → M_{rreq}

N broadcast M_{rreq} to all neighbouring way node(W)

while W_i is not destination node → D_{add} **do**

W_i *Decrypt(M_{rreq})* using CA_{pvt_key} → *[S_{m_sign} , E_{msg} , S_{SKey} , D_{add}, T]*

W_i *Decrypt(E_{msg})* using CA_{pvt_key} → *Msg*

W_i *Encrypt(Msg)* using SHA1 Algorithm → IS_{m_sign}

If *validateSignature (IS_{m_sign} , S_{m_sign}) == true* **then**

If *Msg* == '*RREQ*' **then**

If $W_i == D_{add}$ **then**

D Store Source Session Key(S_{SKey}) → *Destination_Table*

Destination Node D → *Init_Reply(D_{add})*.

Else

W_i Append I_{add} fields data → *Append(M_{rreq}, I_{add})* → M

W_i *Encrypt(M)* using CA_{pub_key} → M_{rreq}

W_i broadcast M_{rreq} to all its neighbouring way nodes (W)

End if

End if

End if

End while

Method2: *Init_Reply(Destadd)*

D Creates Destination Session Key using S_{SKey} and DH Algorithm → D_{SKey}

D *Encrypt(Msg)* using SHA1 Algorithm → D_{m_sign}

D *Encrypt(Msg)* using CA_{pub_key} → E_{msg}.

D *Encrypt([D_{m_sign} , E_{msg} , D_{SKey} , S_{add}, S_{Path} , T])* using CA_{pub_key} → M_{rrep}

D unicast M_{rrep} to the way node (W) from which it recieve RREQ.

while W_i is not source node → S_{add} **do**

W_i *Decrypt*(M_{rrep}) using CA_{pvt_key} -> *M as* [D_{m_sign} , E_{msg}, D_{SKey} , S_{add}, S_{Path} , *T*]

W_i *Decrypt*(E_{msg}) using CA_{pvt_key} → *Msg*

W_i *Encrypt(Msg)* using SHA1 Algorithm → IS_{m_sign}

If *validateSignature* (IS_{m_sign} , D_{m_sign}) == *true* **then**

If *Msg* == '*RREP*' **then**

If $W_i == S_{add}$ **then**

Source Node *N* store destination Session Key(D_{SKey}) → *Routing_Table*

Else

W_i Read Source Path from *M* → S_{Path}

W_i Read next hop from the S_{Path} → $Next_{Hop}$

W_i unicast M_{rrep} → $Next_{Hop}$ (W_i)

End if

End if

End if

End while

3.3 Secure routing mechanism

On successful completion of the secure route discovery, the source node sends the data packets on the optimal route that is stored in the routing table. Generally, the AODV protocol maintains only one route between the source and the destination. In our scheme also, we maintain the same. This is due to the fact that in multi- route discovery, the expenses get increased with the storing of more route information. Before sending the data packet, the source should make the data packets secure.

To do so, the source node generates a unique secret key as SC_{Key} using the destination Session Key, D_{SKey} of DH algorithm that is received during the route discovery process. It encrypts the data packets using SC_{Key} and routes the packets. Using this mechanism, the SWR protocol is capable of securing its data packets during data routing in a feasible route. The mechanism achieved using method 1 and method 2 of secure data routing is described in Algorithm 2.

Algorithm 2: SWR Secure Data Routing Mechanism

Source node *N* init data transmission -> *SendData*(D_{add}, *pkt_seq_no*)

Method1: ***SendData(Destination$_{add}$)***

N gets the discovered route → R_{Path}

N gets destination Session Key → D_{SKey}

N generate unique Secret key using D_{SKey} → SC_{Key}

For "number of data packet to send" **loop**

N creates Data Packet → D_{pack}

N Encrypt data packet using secret key -> *Encrypt* (D_{pack} , SC_{Key}) → E_M

N sends encrypted data packet E_M → $Next_{Hop}$

While *"ACK_Time expires"* **do**

If "*Receive Message* → E_M" **then**

N gets its own Session Key → S_{SKey}

S generate unique Secret key using S_{SKey} → SC_{Key}

S decrypt the data packets using SC_{Key} → *Decrypt*(E_M, S_{SKey}) → D_M

End If

If D_M =="*DELV_ACK*" **then**

End while;

Send next data packet → *SendData*(D_{add}, *pkt_seq_no*)

Else if *"ACK_Time expires"* **then**

Resend the data packet → *SendData*(D_{add}, *pkt_seq_no*)

End if

End while

End for

Method2: ***RecieveData(E_M, pkt_seq_no)***

D gets its own Session Key → D_{SKey}

D generate unique Secret key using D_{SKey} → SC_{Key}

D decrypt the data packets using SC_{Key} → *Decrypt*(E_M, D_{SKey}) -> D_M

D gets its Source Session Key → S_{SKey}

D generate unique Secret key using S_{SKey} → SC_{Key}

D decrypt the *DELV_ACK* message using SC_{Key} → *Decrypt*(*DEL_ACK*, D_{SKey}) → E_M

D Sends secure acknowledge E_M back to source.

3.4 Security investigation

This section investigates the possible attacks [50] in the route discovery process and routing as well as the

countermeasures taken in the SWR to secure routing in mobile adhoc network.

3.4.1 Attacks in route discovery process

- *Route message modification* the process of route discovery requires the intermediate nodes to cooperate to discover the route that reaches the destination. An attack on the intermediate nodes may lead to route message modification.

To handle this kind of attack, the SWR encrypts the route message symmetrically using the SH1 algorithm and asymmetrically using the node's public key. It provides a double shielding for the attackers to pass through, while they perform route message modification and this serves as the novel contribution of this work.

- *Route cache poisoning* This kind of attack misguides the node to route the data in an incorrect path. The SWR handles this attack using the session key that is created by both the source and the destination. A malicious node's broadcast in incorrect paths will have no effect on the route cache. At first, each route requests the message that is highly secured and protected using the session key and the node's public key. Secondly, the unique session key makes the message to be completely different from the regular route message.
- *Not participating in discovery process* Not participating in route discovery or dropping a packet is a passive malicious attribute that will not interrupt the discovery process, until there are non-malicious nodes available in the network. To handle this kind of behaviour, the SWR ensures that each participating node must have an identity and a CA certificate.

3.4.2 Attacks in data routing process

- *Data packet modification* During data communication, it is always possible that the intermediate node can introduce false route through modifying the data packet information and allows the throughput to be degraded. The SWR handles data packet modification through the encryption of data packets using the unique secret key during routing. Both the source and the destination nodes create the unique secret key for sending their data packets and informing the acknowledgement messages.
- *Data packet dropping* Data packet dropping is a common behavior of the malicious nodes, which impact the performance of the network. To handle this kind of attack, the SWR protocol ensures that only a trusted and a CA certified node must participate in the communication process.

4 Experimental evalaution

To evaluate the proposed protocol, we assume that both the internal and the external types of malicious nodes exist. However, we also assume that most of the nodes present in the network are trustable due to the certification acquisition form CA. We use the node's public key cryptography to protect the network against the external attacks and the symmetric cryptography encryption for data and message protection from the internal attacks.

We experimentally simulate the SWR protocol using the Glomosim Simulator [51] to evaluate the performance. It provides a scalable and a parameter driven environment for the wireless protocol simulation. We compare the performances of SWR with SAODV [52], SRAODV [37] and ARAN [36] for evaluation.

4.1 Simulation setup

To simulate the protocol, we setup the parameters that are described in Table 1.

The simulation runs on the Random Way-point model with a speed variation of up to 100 m/s. We perform the simulation in two sets. The first set does not have any malicious nodes, while the second set contains 40 % of malicious nodes.

During the route discovery process, all the nodes behave normally as they are certified. During data routing, we configure the simulator to randomly choose 40 % of the nodes as malicious. It was observed that those nodes, which behave abnormally, try to modify the data packets and drops all the data packets that are routed through them.

Table 1 Simulation parameters

Configuration	Parameter values
Simulation area	1000 m × 1000 m
No. of nodes	50
Pause time	30 s
Source–destination Pairs	25
Packet size	512 bytes
CBR rates	4 pkts/s
Mobility	RWP
Mobility speed (m/s)	0, 20, 40, 60, 80, 100

4.2 Performance analysis

4.2.1 Throughput

Figure 1 shows the throughput performance of the protocol. All the protocols show similar results in the absence of malicious nodes. The SWR shows an improvisation, when compared to the other protocols in the presence of malicious nodes. The improvisation in the throughput is due to the efficient securing of the data packets from attacks. In the absence of malicious nodes, it shows an average performance due to the cryptography overhead. The SWR achieves 25 % improvisation in packet delivery, when compared to the other protocols. The other protocols show a downfall of 10–20 %, when 40 % of malicious nodes are present.

4.2.2 End-to-end delay

Figure 2 shows the end-to-end delay comparison between SWR and other protocols. All the protocols show similar ratio of increase in delays with increase in the mobility speed during the absence of malicious nodes. But, in case of malicious nodes' presence, the SWR and the ARAN show low delays in comparison to other protocols. Both the ARAN and the SWR follow the process of certificate acquisition, which allows secure and identified node in network to minimize packet drop and end-to-end delay in case of malicious attacks.

4.2.3 Routing overhead

Figure 3 shows the comparison of routing overhead between the SWR and others protocols. In the absence of malicious nodes, all the protocols have similar ratio of overhead. But, in case of malicious nodes' presence, the SWR shows low routing overhead in comparison to others. This is because the SWR encrypts and decrypts the data packets only at the source end and the destination the end during data communication. On the other hand, in the other protocols, the security checks are performed during communication and the routing overhead gets increased.

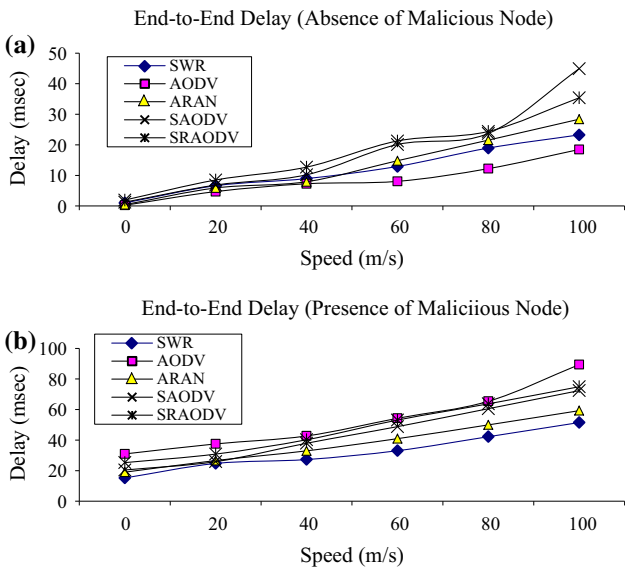

Fig. 2 End-to-end delay performance of the proposed protocol, **a** with no malicious nodes and **b** 40 % malicious nodes

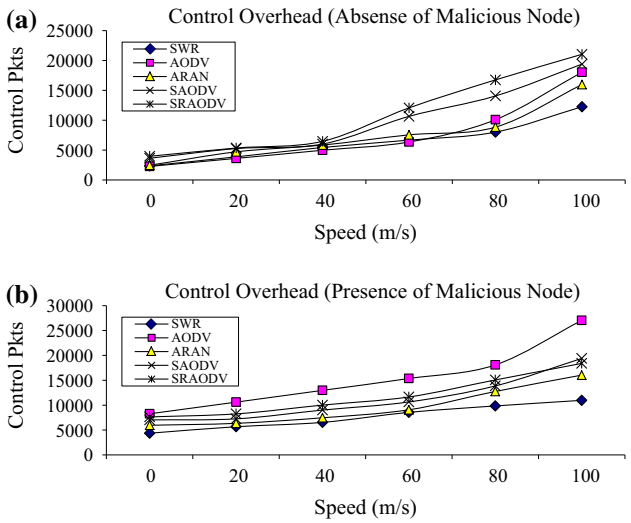

Fig. 3 Control overhead performance of the proposed protocol, **a** with no malicious nodes and **b** 40 % malicious nodes

4.3 Statistical analysis

A statistical analysis has been performed to demonstrate the reliability of the proposed protocol. With the similar experimental setup, we have executed the protocol 100 times. Since the mobility follows RWP plan, every execution produces different performance metrics. These metrics have been obtained and they are subjected to basic statistical functions such as mean, median, best, worst and standard deviation. However, the experimentation is carried out, when the mobile velocity is set to 100 m/s. The results are tabulated in Tables 2, 3, and 4.

Here, each protocol is ranked based on the accomplished statistical metrics. For instance, SWR is ranked one in mean values of Table 2, because its mean throughput is higher than the other protocols. Similarly, for every function a rank is assigned and the average rank is determined at the end of the metrics. The final rank for each protocol is determined based on the average rank. This final rank provides a near substantial performers and non-performers.

Under both no attack and 40 % attack constraints, SWR secures first rank except the throughput measures under no

Table 2 Statistical analysis on throughput at node speed 100 m/s

Attack	Statistical metrics	SWR	AODV	ARAN	SAODV	SRAODV
No attack	Mean (%)	67.16 (1)	66.11 (2)	63.63 (3)	61.58 (5)	62 (4)
	Median (%)	67 (1)	66 (2)	64 (3)	62 (4)	62 (4)
	Best (%)	70 (1)	67 (2)	66 (3)	62 (5)	63 (4)
	Worst (%)	64 (2)	65 (1)	61 (3)	61 (3)	61 (3)
	Standard deviation	2.06 (5)	0.78 (2)	1.77 (4)	0.50 (1)	0.85 (3)
	Average rank	2 (2)	1.8 (1)	3.2 (3)	3.6 (4)	3.6 (4)
40 % malicious attacks	Mean (%)	47.08 (1)	16.17 (5)	43.55 (2)	41.52 (4)	41.95 (3)
	Median (%)	47 (1)	16 (5)	43 (2)	42 (3)	42 (3)
	Best (%)	50 (1)	17 (5)	46 (2)	42 (4)	43 (3)
	Worst (%)	44 (1)	15 (5)	41 (2)	41 (2)	41 (2)
	Standard deviation	2.12 (5)	0.78 (2)	1.67 (4)	0.50 (1)	0.85 (3)
	Average rank	2 (1)	4.4 (5)	2.4 (2)	2.8 (3)	2.8 (3)

Table 3 Statistical analysis on end-to-end delay at node speed 100 m/s

Attack	Statistical metrics	SWR	AODV	ARAN	SAODV	SRAODV
No attack	Mean (s)	15.79 (2)	10.90 (1)	26 (3)	35.95 (4)	51.54 (5)
	Median (s)	16 (2)	11 (1)	25 (3)	36 (4)	52 (5)
	Best (s)	11 (2)	6 (1)	21 (3)	31 (4)	46 (5)
	Worst (s)	21 (2)	16 (1)	31 (3)	41 (4)	56 (5)
	Standard deviation	3.25 (4)	3.02 (2)	3.33 (5)	2.88 (1)	3.12 (3)
	Average rank	2.4 (2)	1.2 (1)	3.4 (3)	3.4 (3)	4.6 (5)
40 % Malicious attacks	Mean (s)	41.13 (1)	90.21 (5)	51.48 (2)	70.87 (4)	70.57 (3)
	Median (s)	41 (1)	90 (5)	52 (2)	70 (3)	70 (3)
	Best (s)	36 (1)	81 (5)	41 (2)	61 (3)	61 (3)
	Worst (s)	46 (1)	101 (5)	61 (2)	81 (3)	81 (3)
	Standard deviation	3.25 (1)	6.27 (3)	5.94 (2)	6.76 (5)	6.27 (3)
	Average rank	1 (1)	4.6 (5)	2 (2)	3.6 (4)	3 (3)

Table 4 Statistical analysis on control overhead at node speed 100 m/s

Attack	Statistical metrics	SWR	AODV	ARAN	SAODV	SRAODV
No attack	Mean	12,624.03 (1)	17,508.29 (3)	14,971.64 (2)	17,576.95 (4)	22,758.58 (5)
	Median	12,497 (1)	17,368 (4)	14,986 (2)	17,303 (3)	22,790 (5)
	Best	10,134 (1)	15,114 (3)	12,116 (2)	15,119 (4)	20,205 (5)
	Worst	15,041 (1)	20,095 (4)	18,012 (2)	20,093 (3)	25,093 (5)
	Standard deviation	1468.40 (2)	1474.28 (3)	1740.88 (5)	1543.32 (4)	1421.19 (1)
	Average rank	1.2 (1)	3.4 (3)	2.6 (2)	3.6 (4)	4.2 (5)
40 % Malicious attacks	Mean	8569.70 (1)	27,549.49 (5)	12,858.78 (2)	17,517.93 (4)	17,490.50 (3)
	Median	8714 (1)	27,435 (5)	12,963 (2)	17,351 (3)	17,475 (4)
	Best	5124 (1)	25,228 (5)	10,105 (2)	15,131 (4)	15,119 (3)
	Worst	12,079 (1)	30,097 (5)	15,096 (2)	20,093 (4)	20,026 (3)
	Standard deviation	2082.18 (5)	1443.72 (2)	1510.36 (4)	1419.99 (1)	1483.61 (3)
	Average rank	1.2 (1)	4.4 (5)	2.4 (2)	3.2 (3)	3.2 (3)

attack condition. Despite AODV secures first rank in this condition, it has secured last rank under 40 % malicious attacks. This raises the question about the robustness of the protocol. However, SWR is proven under insecure environment also.

5 Conclusion and future work

We have presented the secure way routing (SWR) protocol for mobile ad hoc network, which secure the routing mechanism from both the internal and the external attacks.

It has authenticated the route discovery messages using the public key cryptography and has secured the data routing packets using the symmetric cryptography that has made use of the unique session key and the secret key. The experimental evaluations of SWR have shown an improvisation in throughput and routing overhead in case of malicious nodes' presence in the network, when compared with AODV, SAODV, SRAODV and ARAN. It provides a novel contribution through providing a double shielded security to the routing message and the data packets and hence, the attackers find difficulty in intruding

An enhancement to the protocol can be made in the future to evaluate more sensitive parameters of the protocol, which can affect the cryptography process. From the simulation, it was also observed that the effects of mobility have high impact on the performance of mobile adhoc network. So, one can enhance the protocol in future to handle link failure and to repair the process.

References

1. Zhou, J., Cao, Z., Dong, X., Xiong, N., & Vasilakos, A. V. (2015). 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Information Sciences, 314*, 255–276.
2. He, D., Chen, C., Chan, S., Bu, J., & Vasilakos, A. V. (2012). ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE Transactions on Information Technology in Biomedicine, 16*(4), 623–632.
3. Zhou, J., Dong, X., Cao, Z., & Vasilakos, A. V. (2015). Secure and privacy preserving protocol for cloud-based vehicular DTNs. *IEEE Transactions on Information Forensics and Security, 10*(6), 1299–1314.
4. Zhou, L., Xiong, N., Shu, L., Vasilakos, A., & Yeo, S. (2010). Context-aware middleware for multimedia services in heterogeneous networks. *IEEE Intelligent Systems, 25*(2), 40–47.
5. Vasilakos, A. V., Li, Z., Simon, G., & You, W. (2015). Information centric network: Research challenges and opportunities. *Journal of Network and Computer Applications, 52*, 1–10.
6. Lacuesta, R., Lloret, J., Garcia, M., & Peñalver, L. (2013). A secure protocol for spontaneous wireless ad hoc networks creation. *IEEE Transactions on Parallel and Distributed Systems, 24*(4), 629–641.
7. Mukesh, M., & Rishi, K. R. (2010). Security aspects in mobile ad hoc network (MANETs): Technical review. *International Journal of Computer Applications, 12*(2), 37–43.
8. Youssef, M., Ibrahim, M., Abdelatif, M., Chen, L., & Vasilakos, A. V. (2014). Routing metrics of cognitive radio networks: A survey. *IEEE Communications Surveys and Tutorials, 16*(1), 92–109.
9. Yang, M., Li, Y., Jin, D., Zeng, L., Wu, X., & Vasilakos, A. V. (2015). Software-defined and virtualized future mobile and wireless networks: A survey. *Mobile Networks and Applications, 20*(1), 4–18.
10. Zhang, X. M., Zhang, Y., Yan, F., & Vasilakos, A. V. (2015). Interference-based topology control algorithm for delay-constrained mobile ad hoc networks. *IEEE Transactions on Mobile Computing, 14*(4), 742–754.
11. Vasilakos, A. V., Zhang, Y., & Spyropoulos, T. (2012). *Delay tolerant networks: Protocols and applications*. Boca Raton: CRC Press.
12. Zhou, L., Chao, H. C., & Vasilakos, A. V. (2011). Joint forensics-scheduling strategy for delay-sensitive multimedia applications over heterogeneous networks. *IEEE Journal on Selected Areas in Communications, 29*(7), 1358–1367.
13. Fadlullah, Z. M., Taleb, T., Vasilakos, A. V., Guizani, M., & Kato, N. (2010). DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis. *IEEE/ACM Transactions on Networking, 18*(4), 1234–1247.
14. Yao, G., Bi, J., & Vasilakos, A. V. (2015). Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter. *IEEE Transactions on Information Forensics and Security, 10*(3), 471–484.
15. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of things. *Journal of Network and Computer Applications, 42*, 120–134.
16. Liu, B., Bi, J., & Vasilakos, A. V. (2014). Toward Incentivizing anti-spoofing deployment. *IEEE Transactions on Information Forensics and Security, 9*(3), 436–450.
17. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501.
18. Liu, J., Li, Y., Wang, H., Jin, D., Su, L., Zeng, L., & Vasilakos, T. (2016). Leveraging software-defined networking for security policy enforcement. *Information Sciences, 327*, 288–299.
19. Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE Transactions on Mobile Computing, 6*(5), 488–502.
20. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wireless Communications, 11*(1), 38–47.
21. Busch, C., Kannan, R., & Vasilakos, A. V. (2012). Approximating congestion + dilation in networks via "quality of routing" games. *IEEE Transactions on Computers, 61*(9), 1270–1283.
22. Dvir, A., & Vasilakos, A. V. (2010). Backpressure-based routing protocol for DTNs. *ACM SIGCOMM Computer Communication Review, 40*(4), 405–406.
23. Yang, H., Zhang, Y., Zhou, Y., Fu, X., Liu, H., & Vasilakos, A. V. (2014). Provably secure three-party authenticated key agreement protocol using smart cards. *Computer Networks, 58*, 29–38.
24. Yen, Y. S., Chao, H. C., Chang, R. S., & Vasilakos, A. (2011). Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. *Mathematical and Computer Modelling, 53*(11–12), 2238–2250.
25. Yan, Z., Zhang, P., & Vasilakos, A. V. (2015). A security and trust framework for virtualized networks and software-defined networking. *Security and Communication Networks*. doi:10.1002/sec.1243.
26. Khalil, I., & Bagchi, S. (2011). Stealthy attacks in wireless ad hoc networks: detection and countermeasure. *IEEE Transactions on Mobile Computing, 10*(8), 1096–1112.
27. Wei, L., Zhu, H., Cao, Z., Jia, W., & Vasilakos, A. V. (2010). SecCloud: Bridging secure storage and computation in cloud. In *Proceedings of the IEEE 30th international conference on distributed computing systems workshops (ICDCSW)*, June 2010.
28. Attar, A., Tang, H., Vasilakos, A. V., Yu, F. R., & Leung, V. C. M. (2012). a survey of security challenges in cognitive radio networks: Solutions and future research directions. *Proceedings of the IEEE, 100*(12), 3172–3186.

29. Li, P., Guo, S., Yu, S., & Vasilakos, A. V. (2012). CodePipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding. In *Proceedings of the IEEE INFOCOM*, March 2012.
30. Li, P., Guo, S., Yu, S., & Vasilakos, A. V. (2014). Reliable multicast with pipelined network coding using opportunistic feeding and routing. *IEEE Transactions on Parallel and Distributed Systems, 25*(12), 3264–3273.
31. Wang, T., Liu, Y., & Vasilakos, A. V. (2015). Survey on channel reciprocity based key establishment techniques for wireless systems. *Wireless Networks, 21*(6), 1835–1846.
32. Zeng, Y., Xiang, K., Li, D., & Vasilakos, A. V. (2013). Directional routing and scheduling for green vehicular delay tolerant networks. *Wireless Networks, 19*(2), 161–173.
33. Meng, T., Wu, F., Yang, Z., Chen, G., & Vasilakos, A. (2015). Spatial reusability-aware routing in multi-hop wireless networks. *IEEE Transactions on Computers, 99*, 1.
34. Perkins, C. E., Royer, E. M., & Das, S. R. (2003). Ad hoc *on-demand distance vector (AODV) routing*. IETF Internet draft, MANET working group, February 2003.
35. Johnson, D. B., Maltz, D. A., & Hu, Y. C. (2004). *The dynamic source routing protocol for mobile ad hoc networks (DSR)*. IETF Internet draft, MANET working group, July 2004.
36. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Royer, E. M. (2002). *A secure routing protocol for ad hoc networks (pdf)*. Technical Report: UM-CS-2002-032, 2002.
37. Zapata, M. G., & Asokan, N. (2002). Securing ad hoc routing protocols. In *Proceedings of the 1st ACM workshop on Wireless security*, September 2002.
38. Pirzada, A., & McDonald, C. (2005). Secure routing with the AODV protocol. *In Proceedings of the Asia-Pacific conference on communications*, October 2005.
39. Yu, W., Sun, Y., & Liu, K. J. R. (2005). HADOF: Defense against routing disruption in mobile ad hoc networks. In *Proceedings of the 24th annual joint conference of the IEEE computer and communications societies (INFOCOM 2005)*, March 2005.
40. Yu, W., Sun, Y., & Liu, K. J. R. (2005). Stimulating cooperation and defending against attacks in self-organized mobile ad hoc networks. In *Proceedings of the second annual IEEE communications society conference on sensor and ad hoc communications and networks (SECON'05)*, September 2005.
41. Zhu, S., Xu, S., Setia, S., & Jajodia, S. (2006). LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks. *Ad Hoc Networks, 4*(5), 567–585.
42. Yan, J., Ma, J., Li, F., & Moon, S. J. (2010). Key pre-distribution scheme with node revocation for wireless sensor networks. *Ad Hoc and Sensor Wireless Networks, 10*(2/3), 235–251.
43. Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2005). Authenticated routing for ad hoc networks. *IEEE Journal on Selected Areas in Communications, 23*(3), 598–610.
44. Luo, H., Zerfos, P., Kong, J., Lu, S., & Zhang, L. (2002). Self-securing ad hoc wireless networks. In *Proceedings of the seventh international symposium on computers and communications (ISCC 2002)*, July 2002.
45. Abedi, O., & Fathy, M. (2008). Enhancing AODV routing protocol using mobility parameters in VANET. In *Proceedings of the IEEE/ACS international conference on computer systems and applications (AICCSA 2008)*, March/April 2008.
46. Papadimitratos, P., & Haas, Z. (2002). Secure routing for mobile ad hoc networks. In *Proceedings of the SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002)*, January 2002.
47. Asokan, N., & Ginzboorg, P. (2000). Key agreement in ad-hoc networks. *Computer Communication Review, 23*, 1627–1637.
48. Kong, J., Zerfos, P., Luo, H., Lu, S., & L. Zhang. (2001). Providing robust and ubiquitous security support for wireless mobile networks. In *Proceedings of ninth international conference on network protocols*, November 2001.
49. Xiao, Y., Rayi, V. K., Sun, B., Du, X., Hu, F., & Galloway, M. (2007). A survey of key management schemes in wireless sensor networks. *Computer Communications, 30*(11/12), 2314–2341.
50. Sahadevaiah, K., & Prasad Reddy, P. V. G. D. (2011). Impact of security attacks on a new security protocol for mobile ad hoc networks. *Network Protocols and Algorithms, 3*(4), 122–140.
51. Zeng, X., Bagrodia, R., & Gerla, M. (1998). GloMoSim: A library for parallel simulation of large-scale wireless networks. In *Proceedings of twelfth workshop on parallel and distributed simulation*, May 1998.
52. Kumar, V., & Das, M. L. (2008). Securing wireless sensor networks with public key techniques. *Ad Hoc and Sensor Wireless Networks, 5*(3/4), 189–201.

Jarupula Rajeshwar is working as Associate Professor and Head of the department in the department of Computer Science and Engineering of Vijay Rural Engineering College. Nizamabad, T.S. He has more than 14 years of teaching experience. He obtained his B.Tech, in Computer Science and Engineering from JNTU College of Engineering JNTU Hyderabad in the year 2000 and M.Tech, in Computer Science and Engineering from Osmania University College of Engineering OU Hyderabad with distinction and presently pursuing his research work (Ph.D.) from JNTUH College of Engineering, JNTUH, Hyderabad in the area of Computer Networks. He published six international journals, four national journals and published his five papers in international conferences. He conducted a couple of short term courses, seminars, workshops and delivered few expert lectures. He is expert in guiding projects for under graduate and post graduate students, guiding students for paper presentation, project exhibition and poster presentation.

Gugulotu Narsimha is working as Associate Professor in the department of CSE at JNTUH College of Engineering, Nachupally, Karimnagar, T.S. and he has about 16 years of teaching experience. He obtained B.E. in Electronics and Communication Engineering, University College of Engineering, Osmania University Hyderabad, A.P. India, in the year of 1996, M.Tech in Computer Science and Engineering, University College of Engineering, Osmania University Hyderabad, A.P. India, in the year of 1999, Ph.D. in Computer Science and Engineering, University College of Engineering, Osmania University Hyderabad, A.P. India, in the year of 2009. He published more than eighty international/national journals, fifty national/international conferences.