Gunasekaran and Premalatha *EURASIP Journal on Wireless Communications and Networking* 2013, **2013**:220
http://jwcn.eurasipjournals.com/content/2013/1/220

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

SPAWN: a secure privacy-preserving architecture in wireless mobile ad hoc networks

Muthumanickam Gunasekaran* and Kandhasamy Premalatha

Abstract

Fourth-generation wireless networks may require an integration of mobile ad hoc networks (MANET) into external network to enhance the flexibility of the communication and roaming. This phenomenon is well-suited for commercial and military applications which yield additional benefit of roaming. However, integration of MANET with external network poses a serious security challenge for communication because of open and distributed nature of the ad hoc network. In this paper, a secure privacy preserving architecture has been proposed to provide privacy and security for data communication in wireless mobile ad hoc networks. This architecture includes the concept of observer obscurity to provide privacy and security for the genuine nodes and to exclude misbehaving nodes in the network. The proposed architecture is designed based on the k-times anonymous authentication and onion routing - a cryptography concept which supports for anonymous communication. The simulation results prove the necessity and effectiveness of the proposed architecture in achieving such privacy and security in the integrated environment.

Keywords: Trust; Security; Privacy; Obscurity and routing

1. Introduction

The evolution of fourth-generation (4G) wireless networks integrates mobile ad hoc networks (MANET) with other networks such as cellular networks, wireless local area networks (LANs) and third-generation (3G) systems to enhance the flexibility in communication. The major goal of 4G network is to allow mobile nodes to roam globally without any limit to underlying technologies [1-3]. One of the emerging categories of wireless network called MANET is included in the 4G systems.

MANET is a collection of mobile hosts which utilize multi-hop radio relaying and are capable of operating without any fixed infrastructure. The lack of fixed infrastructure in ad hoc networks causes nodes to rely more heavily on peer nodes for communication [4]. The nodes have the ability to configure themselves and form a temporary ad hoc topology. MANETs were initially used to operate as standalone networks for ad hoc communications, such as conferences, emergency rescue or military missions, restricting its traffic within its [5] limitation. Unlike traditional fixed Internet Protocol (IP) networks, all users in a MANET communicate over multi-hop relays by equally distributing and maintaining the routing information by running the same ad hoc routing protocols [6]. This behavior differentiates the MANET nodes with the nodes in other networks.

* Correspondence: sangraghav@gmail.com
Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India

So far, most of the research work is done on protocols for autonomous mobile ad hoc networks. During the last few years, some work has been done concerning with the integration of mobile ad hoc networks with other networks for the purpose of internet access [7,8]. The purpose of this integration with other networks, like the internet, is to allow the ad hoc nodes to communicate with any part of the world. The 4G networks provide such an opportunity for mobile ad hoc networks [9] to maintain global connectivity without any interruption for ongoing connection paths and also the MANET may help to extend the coverage of existing infrastructure networks, like wireless LANs and 3G networks.

4G networks are envisioned as hybrid broadband networks that integrate different network topologies and standards. In Figure 1, the overlapping of different network boundaries represents the integration of different types of networks in 4G. There are two levels of integration. First is the integration of heterogeneous wireless networks with varying transmission characteristics such as cellular networks, wireless LAN as well as mobile ad hoc networks. At the second level, wireless networks are integrated with the fixed network backbone infrastructure, the internet, and PSTN. Much work remains to enable a seamless integration, for example extending IP or IP extension to support mobile network devices.

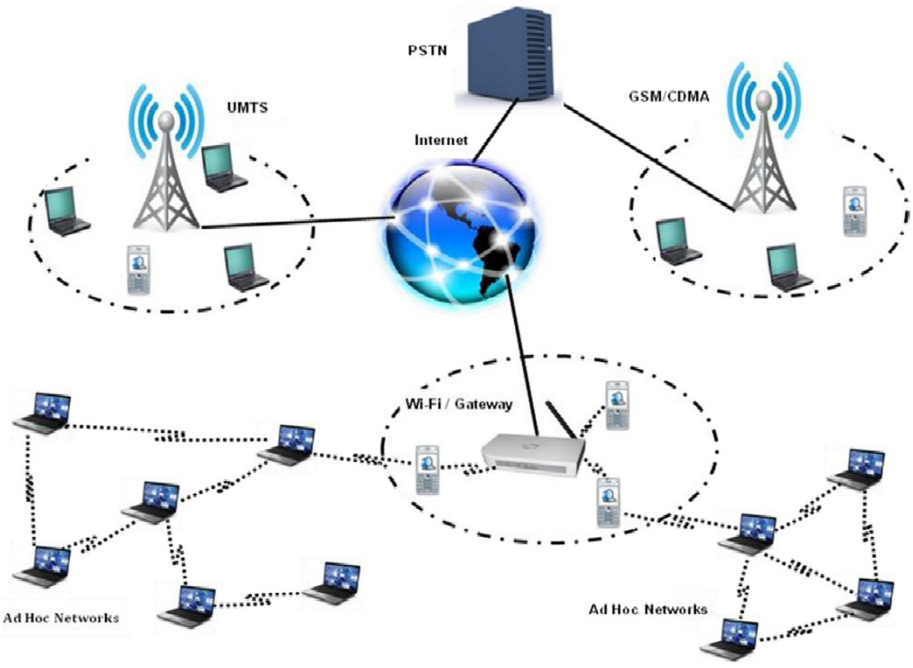

Figure 1 4G networks.

However, connecting MANETs to the external network for internet access pose serious threats and challenges [10,11]. Normally, the interoperability is different for ad hoc routing protocols than the regular routing protocols used in the internet. The ad hoc routing protocols participate on the route learning and maintenance in ad hoc networks whereas in the internet, these tasks are left to specialized routers running routing protocols. Communication between nodes on the internet and mobile ad hoc nodes is done throughout specialized mobile gateways (MG) that are located at the edge of a MANET and provide connections to both, the infrastructure network and the MANET. So, the MG must run the routing protocol used in the infrastructure network and the ad hoc routing protocol used in the MANET to provide an interface between both the networks. The MG takes the responsibility in integrating MANET with internet through Mobile IP which enables flexibility in communication across the network. Mobile IP defines the functional entities such as Home Network, Home Agent, Foreign Network, Foreign Agent and Care of Address and the functionalities of these entities are discussed in [12] and the discussion of this part is beyond the scope of this work.

Security plays a major role in integrating MANET and fixed networks for the purpose of accessing the internet in an adverse environment. Integration of Mobile IP and ad hoc networks enables mobile nodes, as well as MG to move between networks while retaining the connectivity to the external network. In these circumstances, consider a battle field environment; the presence of malicious nodes may pose a serious threat to the success of the covert missions because the communication may require two ways: firstly, a node from ad hoc network may want to convey secret information to the other nodes in the same network then the usual ad hoc routing protocols can be used for communication. Secondly, a node may want to surf some important information from the external network; this can be achieved through Mobile IP and MG. This environment creates a provision for misbehaving nodes to induce active or passive attacks in the network in order to exploit the covert missions. There are a number of mechanisms that have been proposed in the past but those protocols are compromised in many ways. So, there is a need of a technique to provide privacy and security for the mobile nodes while communicating between ad hoc networks to fixed network and vice versa.

In this paper, a secure privacy preserving architecture has been proposed to provide privacy and security for data communication in wireless mobile ad hoc networks. This architecture includes the concept of observer obscurity to provide privacy and security for the genuine nodes and to exclude misbehaving nodes in the network. A misbehaving node is categorized as outlier (who drops the data packets instead of forwarding) or malicious (who does not send cooperation message, upon receiving a caution). These nodes are excluded in two ways: firstly, a user is declared as outlier if the overall trust is less than the threshold. Secondly, a user is revealed as malicious if it does not send a cooperation message upon receiving a caution. The proposed architecture is designed based on the k-times

anonymous authentication and onion routing - a cryptography concept that supports for anonymous communication. The k-times anonymous authentication scheme [13] supports the distributed and decentralized nature of wireless ad hoc networks. The cryptographic Trapdoor Boomerang Onion [14] is used to create untraceable paths or packet flows in an on-demand environment with route pseudonymity approach. The design of route pseudonymity is based on "broadcast with trapdoor information" - a cryptography concept. Trapdoor information is used in this paper mainly for encryption and authentication.

The rest of the paper is organized as follows: the related works are discussed in section 2; section 3 discusses the threat model and design goals; preliminaries and communication scenarios are discussed in section 4; the propose architecture is discussed in section 5; section 6 provides the security analyses; section 7 describes simulation environments and presents the simulation results; and section 8 discusses the conclusion.

2. Related works

The ad hoc routing protocols and techniques have been studied extensively for the integration of MANET with fixed network for internet access.

2.1 MANET with fixed network

Daemon is one of the earliest techniques proposed by Sun et al. [12] to integrate the ad hoc routing protocol and Mobile IP routing. But this technique does not discuss about the privacy and security features. Wakikawa et al. [15] investigated the use of ad hoc routing protocols for route-optimized communication between mobile networks. The route has been provided by the ad-hoc routing protocol or by the basic NEMO routing approach itself whenever it is desirable. Jonsson et al. [16] designed a Mobile IP for MANET (MIPMANET) scheme that provides Ad Hoc On-Demand Distance Vector (AODV)-based MANET with access to the internet using Mobile IP. A MIPMANET interworking unit is inserted between a gateway and the MANET.

Broch et al. [17] propose a principle that allows a DSR-based MANET with single gateway to span across heterogeneous link layers. This architecture supports only a single gateway in a MANET IP subnet. Kock and Schmidt [18] proposed dynamic mobile IP routers in ad hoc networks to act as gateways to the rest of the network. Tseng et al. [19] proposed an idea for extending traditional IEEE 802.11-based access points to incorporate the flexibility of mobile ad hoc networks which would help to make the dream of ubiquitous broadband wireless access a reality. Perkins et al. [20] used Mobile IP as the basis for providing mobility for nomadic users, and extend it to facilitate additional services for nomadic users both at the network layer and above.

2.2 Anonymous communication techniques

Anonymous communication protocols are studied extensively in ad hoc networks and most of the works are based on onion routing protocol [21] proposed by Reed et al. in which data is wrapped in a series of encrypted layers to form an onion by a series of proxies communicating over encrypted channels.

There are protocols in MANET which addresses the anonymity-related issues proposed by Kong et al. [14]. An Anonymous On-Demand Routing Protocol (ANODR) is the first one to provide anonymity during route discovery and data forwarding in ad hoc networks. Following the work of ANODR, Seys and Preneel [22] proposed Anonymous Routing Protocol (ARM) which uses one-time public/private key pairs and discusses about only anonymity in route discovery and data forwarding. Sy et al. [23] proposed the On-Demand Anonymous Routing (ODAR) using public key cryptosystems for secure anonymous routing, but they assume that long-term public/private key pairs have been set up on each node for anonymous communication. Zhang et al. [24] proposed the Anonymous On-Demand Routing (MASK) which enables an AODV-like anonymous on-demand routing protocol with high routing efficiency by comparing with ANODR (which is very sensitive to node mobility) and which may lower routing efficiency.

Choi et al. [25] proposed an Anonymous and Secure Random Reporting Protocol for a civilian ad hoc network, in which the source and destination collect reports from intermediate nodes on the routing path. Zhu et al. [26] proposed an Anonymous Malicious Detection Mechanism which provides anonymity for the witness who reports observed malicious to the network anonymously and ignores malicious and selfish users from the group. Pan and Li [27] proposed an Efficient Strong Anonymous Routing Protocol (MASR) which overcomes the problems of ANODR and MASK and provides efficiency, security, strong anonymity, and adaptability for route discovery and data forwarding.

3. Threat model and design goals

This section describes the threat model and the design goals in order to manage the threat posed by misbehaving nodes.

3.1 Threat model

The integration of MANET with fixed network pose a terrible challenge because the functionality of ad hoc routing protocols are quite different from the routing protocols of fixed network. In the fixed network, the nodes do not participate on the route learning and maintenance whereas in mobile ad hoc network, every node must exchange routing information with other nodes within its proximity which makes every node act as an end node or as a router. Communication between nodes in MANET and nodes in the fixed network is

achieved through the routers located at the edge of a MANET called gateways.

This environment poses a serious security threat on MANET than the fixed network.

Being an active part of the network, it is easy for the attackers to exploit any individual or the entire network itself. Passive eavesdroppers do not disrupt the normal operation of the network; instead, they listen to the network in order to extract the cryptographic information. In addition, an attacker may want to gain access to the network or impersonate as a valid entity which gives more challenge for secure communication in the integrated environment.

3.2 Design goals

The design goal of the proposed architecture is to provide the following requirements to identify misbehaving nodes using the trust and reputation metrics and to exclude them from the network:

- Obscurity: It should not be possible for misbehaving users to identify the identity of the observer (who identifies and discloses the outliers/malicious users in the network anonymously).
- Accountability: An observer is liable to identify and reveal the identity of misbehaving users in the network anonymously.

4. Network architecture

4.1 Preliminaries

Since MANETs were envisioned as distributed networks, their nodes are not usually set with addresses. So, the nodes in ad hoc networks should use IP addresses for communication with the nodes in the fixed network for internet access. One convenient way for assigning structured IP addresses to mobile nodes is to use the same network prefix that is used by the closest gateway. When a mobile node moves and selects a different gateway, it configures a new address with the new prefix. With the globally routable address, packets can be received from and sent to the internet. In this way, mobile nodes will be organized as sub-network surrounding these gateways that share the same network prefix. This organization facilitates the routing tasks done by routers on the internet, by mobile nodes in the MANET, and by gateway, which have interfaces facing both types of networks [28]. In summary, a mobile node obtains its globally routable address [29] by following the steps given below:

(a) Has an initial IP address (home address) which is routable in the ad hoc network;
(b) Discovers reachable gateways in its surrounding;
(c) Selects one gateway out of the set of reachable gateways; and
(d) Forms a globally routable IP address with the prefix of the selected gateway.

The gateway discovery is a key component for the MANET nodes in order to communicate with internet hosts. The gateway discovery can be made either by proactive or reactive approach. In proactive approach, periodical gateway advertisements are sent to all nodes in the ad hoc network from the gateways. In the reactive approach, solicitation and advertisement messaging takes place between a mobile node and the gateway. Once a mobile node discovers a gateway, it can connect to the internet through the gateway.

Figure 2 shows the proposed network architecture. Mobile gateways MG-1 and MG-2 connects MANET to the internet, supports Mobile IP and also serves as the local foreign agent. Hereafter, any mobile host that joins the MANET will be served by the gateway.

4.2 Communication scenarios

The proposed network architecture can accommodate two different communication scenarios such as Intra-MANET communication and Inter-MANET communication. This model implements the base specification of the AODV [30] protocol for all corresponding MANET routings.

4.2.1 Intra-MANET communication

AODV supports intra-MANET communications. It implements all functionality of service and discovers routes on demand. The transmission from host S to host D shown in Figure 3 falls into this category. Host S sends packets to host D through AODV.

4.2.2 Inter-MANET Communication

A host in a MANET will forward any packet whose destination is not listed in the routing table to the local MANET's gateway. The gateway will then forward the packet to the internet. The transmission from host S to host D in Figure 4 is an example of this kind of packet transfer. Packets travel on MANET-1 based on AODV, then on the internet to MG-2 based on IP routing, and then again by AODV to host D on MANET-2. When a mobile node roams away from its home network, Mobile IP will forward packets between MANETs. For example, in Figure 4, during packet transmission from the corresponding host to host M, packets arrive at MG-1 via IP routing which then uses AODV to forward them to mobile host M.

5. The SPAWN

The secure privacy-preserving architecture in wireless mobile ad hoc networks (SPAWN) is designed to provide security and privacy for the nodes either in ad hoc networks or in the internet during data communication. There are three entities, i.e. the mobile nodes in ad hoc network, mobile gateway and regular nodes in the fixed network. The system model for the proposed architecture is depicted in Figure 5.

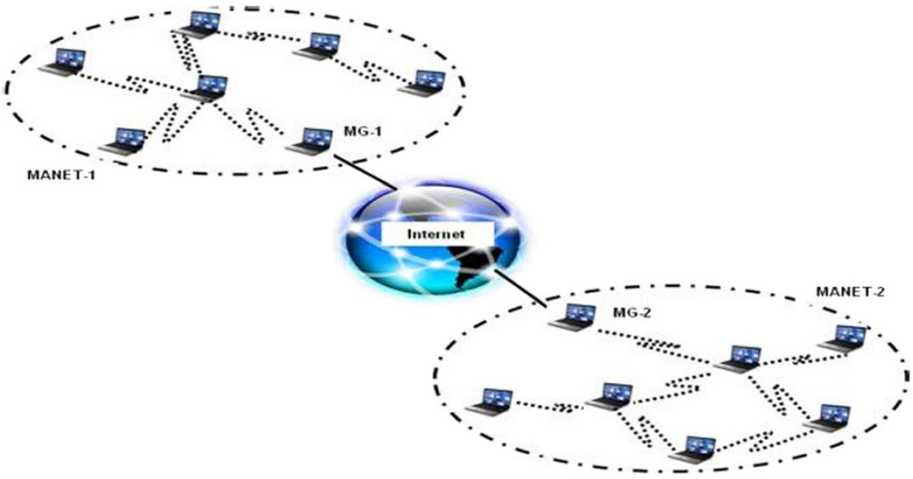

Figure 2 Proposed network architecture.

The components and the functionalities of the SPAWN are described in the following subsections:

5.1 Configuration module

The configuration module has two faces such as the initial setup and the user registration (discussed in [31]).

During the initial setup phase, the MG generates a group key (public/secret key pair) and sends announcement with group public key during gateway advertisement. In addition, MG also publishes the method of generating the tag bases that will be used to send caution, cooperation and event reporting.

5.1.1 Warning

If any user notices malicious activity in the network can act as an observer and send a caution. The format of caution message is as follows:

$$\left(W_k, W_k^{'}\right) = H_{G_T x G_T}\left(W_{msg}, ID_{malicious}, MAX_{caution}, k\right) \quad .....(1) \text{ for } k = 1, ...MAX_{caution}$$

where W_{msg} denotes the caution message that has been sent to the malicious user, $ID_{\mathrm{malicious}}$ denotes the identity of a malicious user and $\mathrm{MAX}_{\mathrm{caution}}$ denotes the maximum number of caution that can be sent malicious user. In this paper, $\mathrm{MAX}_{\mathrm{caution}} = 1$.

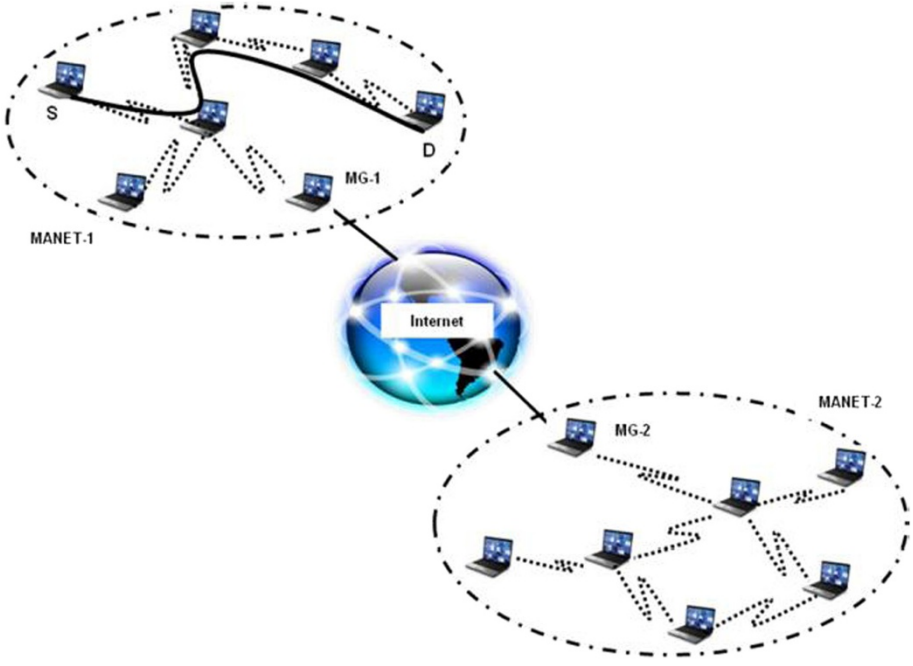

Figure 3 Intra-MANET communication.

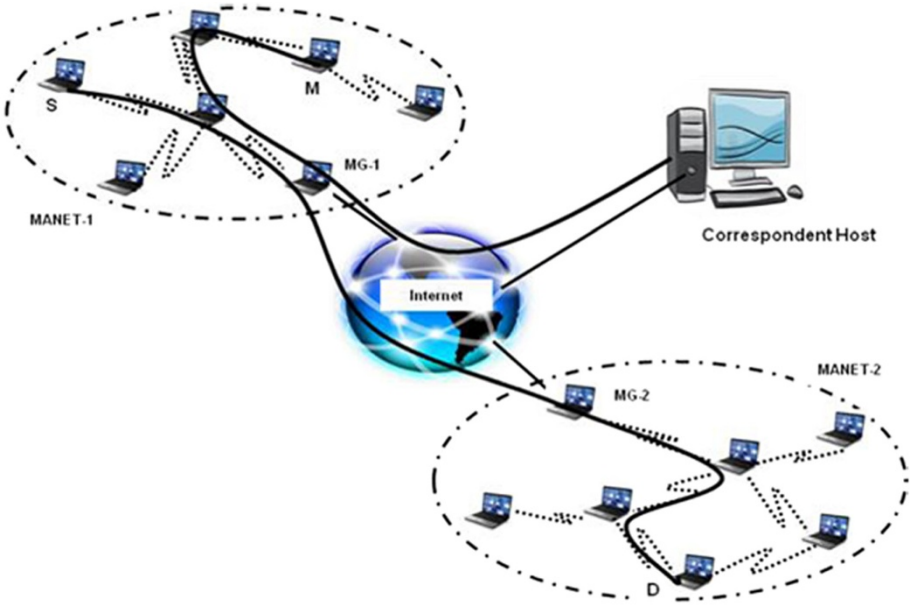

Figure 4 Inter-MANET communication.

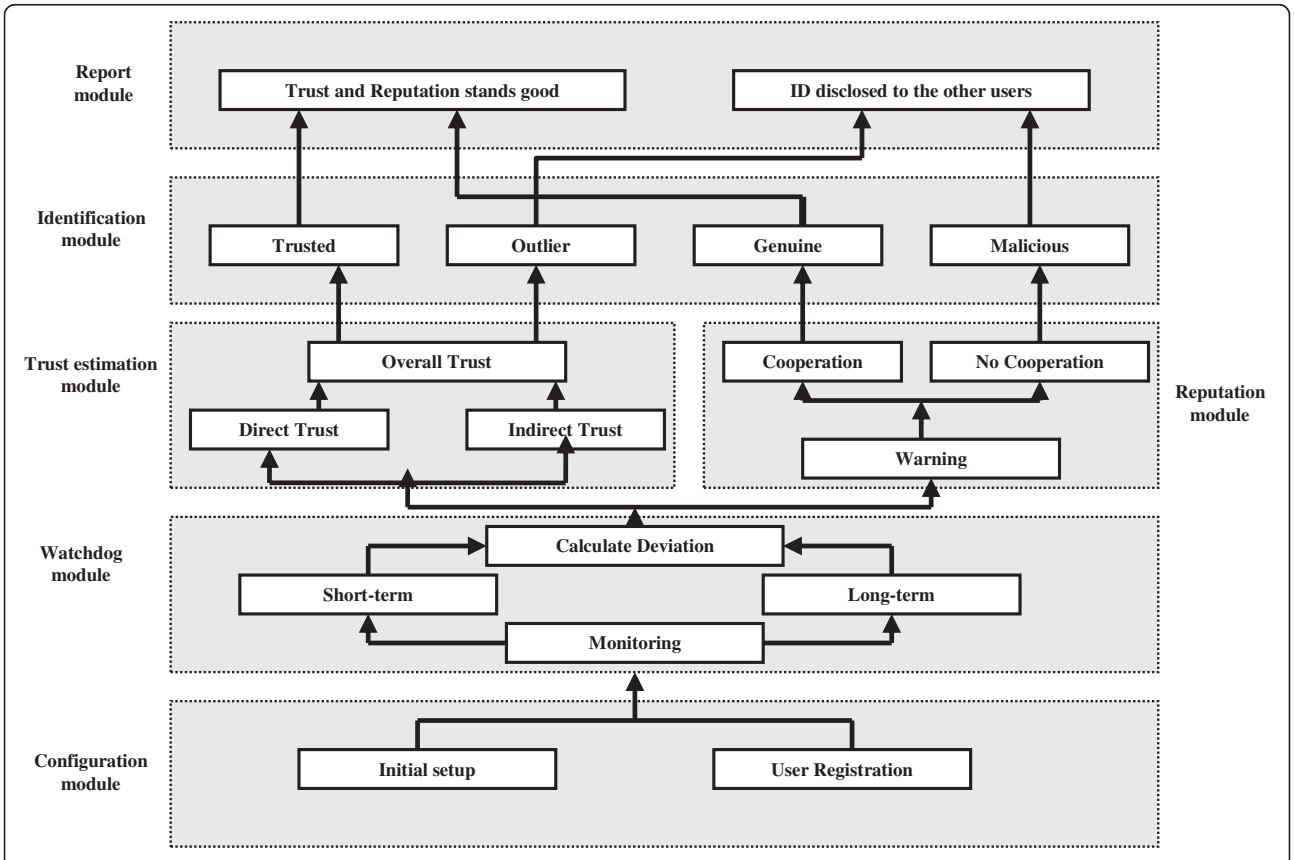

Figure 5 System model of SPAWN.

5.1.2 Cooperation

If any user receives a warning, it has to send a cooperation message at once. The format of cooperation message is follows:

$$\left(E_l, E_l^{'}\right) = H_{G_T x G_T}\left(C_{msg}, ID_{source}, MAX_{cooperation}, l\right) \quad \text{.....(2) for } k = 1, \ldots MAX_{cooperation}$$

where C_{msg} denotes the cooperation message that the user has to send to the initiator of the cooperation message, ID_{source} denotes the identity of the user who sends the caution message and $\text{MAX}_{\text{cooperation}}$ denotes the maximum number of cooperation message that the user can send. In this paper, $\text{MAX}_{\text{cooperation}} = 1$.

5.1.3 Report

Any user identifies an outlier or malicious user in the network which can act as an Observer and report it to the other users. However, an Observer can send report at once. The format is as follows:

$$\left(T_j, T_j^{'}\right) = H_{G_T \times G_T}\left(Type_{event}, ID_{malicious}, MAX_{report}, j\right) \quad \text{.....(3) for } j = 1, \ldots MAX_{report}$$

where $\text{Type}_{\text{event}}$ denotes the type of event that the claim is against, e.g. packet drop or tampering, $ID_{\text{malicious}}$ denotes the identity of the malicious user. $\text{MAX}_{\text{report}}$ denotes the maximum number of report an Observer can send. In this paper, $\text{MAX}_{\text{report}} = 1$.

Pseudo code-1: Initial setup

```
setup()
    begin
        // setup
          input a security parameter 1^k
          generate_tuple (p, G1, GT, e, P)
          MG selects P0, H ∈U G1, γ ∈ Z*p
          Ppub ← γP
          Δ ← e(P, P)
          gpk ← (P, Ppub, P0, H, Δ)
          gsk ← γ
          iLIST ← empty
    end
```

The user who wants to join in the network chooses an identity and sends user registration request to *MG*. After this step, the user obtains a member public/secret key pair, and then the *MG* adds the user's identity and public key to the identification LIST. A user who has completed the registration procedure is called a member of the network.

Pseudo code-2: User registration

```
registration()
    begin
        // registration
          for each user U_i interacts with MG do
          U_i selects the identity and forwards to MG
          repeat
              if i = iLIST then
                choose another identity until
                i != iLIST
                U_i sends commitment
                C' = x'P + rH of x' to MG
                MG sends y, y' ∈∪ Z*p to U_i
                U_i computes x = y + x'y' and
                (C, β) = (xP, Δ^x)
                U_i sends (C, β) to MG with Proof_1
                if Proof_1 is valid and e(C, P) = β
                is satisfied then MG
                  adds (i, β) to iLIST
                  generates a ∈∪ Z*p
                  compute S = (1/(γ + a))(C + P0)
                  sends (S, a) to U_i
                  selects s items from iLIST
                  then send to U_i
                  all iLIST items are signed
                  with MG's secret key
                  else
                    // do nothing
                end
                if e(S, aP − Ppub) = e(C + P0, P)
                is satisfied then
                  U_i obtains secret key u_sk = x and
                  public key u_pk = (a, S, C, β)
                  U_i verifies s iLIST from MG
                end
    end
```

5.2 Watchdog module

The main function of the watchdog module is to overhear the packet transmission and collect useful

information about network behaviors, such as packet forwarding, dropping and tampering. Initially, the user monitors the one-hop neighbor in a short-term monitoring basis. However, if a user finds any malicious activity, it monitors the particular user in a long-term monitoring basis.

Pseudo code-3: Overhearing the node's behavior

```
Watchdog()
    begin
        if sender/forwarder overhears a data packet
        begin
            if expected packets
            begin
                recorded as a forwarded packet
                status(nexthop) = good
            end
            if sent packets Time-Out
            begin
                if count(non-forwarded packet) > threshold
                begin
                    if status(nexthop) != good
                    begin
                        send alarm packet to source
                        status(nexthop) = malicious
                    end
                end
            end
        end
    end
```

5.3 Decision making module

This section describes the process of estimating the trust, judging the reputation and how the mobile nodes are categorized as trusted/outlier and genuine/malicious.

5.3.1 Trust estimation module

This module compares the collected data with the predefined threshold value and finds the deviation. Based on the information collected and compared by the user, it calculates the direct trust value and stores it into the local database DB_{LOC}. The direct trust value is calculated mainly based on the behavior of packet forwarding, dropping and tampering. The indirect trust value is determined based on the information collected from other users in the network and maintained by the common database DB_{COM}.

5.3.2 Reputation module

Any user suspects the malicious activity such as holding the packets for a long time or giving false report in the network is performed by any user, it can send a caution at once to that user. Upon receiving a caution, the genuine user has to send a maximum of one cooperation message using the tag base published in the setup procedure. If the user does not send cooperation (one time) or sends multiple cautions is marked as a malicious user.

5.3.3 Identification module

In this module, the trust value obtained from the trust estimation module is compared with the threshold. If the trust value is less than the threshold, then the user can be marked as outlier otherwise trusted. In the same way, based on the reputation obtained from the reputation module, the user can be marked as malicious or genuine.

Pseudo code-4: Deciding the state of the node

```
node_state ()
    begin
        Q's neighbor P calculates
            packet_received ← Rd_Q
            forwarded_count ← Fd_Q
            RF_Q^P ← (Rd_Q − Fd_Q)/Rd_Q
            RF_Q^P sends to the other nodes
            if RF < RF_threshold
              Q is trusted
            else
              Q is outlier
            if N notices malicious activity
              begin
                  send W_msg to Q
                  if P receives C_msg from Q
                        Q is genuine
                  else
                        Q is malicious
              end
    end
```

5.4 Report module

Any user who identifies an outlier or malicious user in the network can act as an Observer and categorize him/her as a misbehaving user. Then the Observer can report to the other users in the network a maximum of one time per reason per misbehavior type. The claim will be accepted by other users if and only if the Observer is a group member.

Pseudo code-5: Sends a report (discussed in [31])

```
report ()
    begin
      observer selects a random number l ∈∪ Z_p^*.
      compute_tag (Γ, Γ̄) = (T_1^x, Δ'T_1'^x) using (T_1, T_1')
      broadcasts (Γ, Γ̄) with Proof_1 = PROOF((a, S, x))
     //report format [Type_event, ID_event, Γ, Γ̄, l, Proof_1]
     if user receive a claim
       begin
         computes T_1 = H_{G_T xG_T}(Type_ad, ID_ad, Γ, 1, 1)
          if Proof_1 is valid  //there is exists same claim in
          DB_LOC and DB_COM
            //ignores
          else
            records the claim into DB_COM and re-broadcast
          end
       end
       if user found k+1 claims
         mark as misbehaving user
       else
         // no operation
       end

  end
```

6. Security analysis

This section presents an informal analysis on the security- and privacy-related goals. The SPAWN is designed based on the k-times anonymous authentication scheme and onion routing. The k-times anonymous authentication scheme is modified according to ad hoc networks in such a way that it supports privacy and accountability at the same time. The proposed architecture focuses on network layer and the routing process that is route discovery, data forwarding and reporting is based on [4,31]. In addition, Elliptic Curve Digital Signature Algorithm (ECDSA) [32] is used for authentication with the key size of 256 bit. The computational cost signature generation and verification is shown in Table 1.

Table 1 Computational cost

Parameter	Value
ECDSA signature generation	160 ms
ECDSA signature verification	160 ms
Key size	256 bit
Key pair generation time	130 ms
Size	128 bit
Key agreement time	150 ms
Size	64 bit
SHA1	20 ms

6.1 Privacy

In SPAWN, to prevent traffic analysis, an observer sends the caution and report through an anonymous communication system so that misbehaving user could not discover the identity of the sender. There is no public key or identity-related information in a report, and the verification process is based on the zero knowledge proof as discussed in [33].

6.2 Accountability

If a user does not send a cooperation message upon receiving a caution, then he/she is marked as malicious. To ensure a malicious user misusing an obscurity feature, genuine users need to find a valid record of the distinguished user, i.e. in each item in *i*LIST has copies distributed in all the nodes in the network. If a user does not send a cooperation message after receiving caution, then the identity of the user will be revealed to the other users in the networks.

This section also discusses the considerable attacks and present possible countermeasures.

6.2.1 Impersonation attacks

Impersonation attacks are only possible for inside attackers. Even if malicious users compromise multiple users in the network and collect additional report, they cannot differentiate the reports sent by a user from those sent by others. Thus, compromising more users does not increase the probability of deducing the identity of the sender, i.e. the observer obscurity.

6.2.2 DoS attacks

DoS attacks aim to deplete resources, including computation capability, bandwidth, memory, energy, etc. DoS attacks can be initiated from outside attackers as eavesdroppers or inside attackers. In the proposed architecture, DoS attacks can be launched against the event reporting procedure and is restrained by the accountability property.

7. Performance analysis

This section evaluates the performance and effectiveness of the proposed architecture.

7.1 Simulation setup

The proposed technique for MANET is implemented on ns2 simulator version 2.32 and evaluates its performance by comparing with the basic AODV routing protocol and MIPMANET as discussed in the “Related works”

Table 2 Scenario parameters

Parameter	Value
Simulation time	700 s
Scenario dimension	700 m × 700 m
Wireless radio range	250 m
Mobile nodes	100
Node speed	0 to 10 m/s
Traffic type	CBR 512-byte packet
Mobility model	Random Way Point model

section. The network scenario parameters used for simulation are listed in Table 2. In the simulation scenario, an ad hoc network of size 700m × 700m consists of 100 mobile nodes and the node in blue color is OCM and the nod red color is an adversary. Simulation is done with the benchmarks on a 2-GHz Pentium Dual Core platform. The mobile nodes are moving in the field according to the random waypoint model, and their average speeds range from 0 to 10 m/s. The bidirectional constant bit rate (CBR) traffic is generated and the radio range of mobile node is 250 m.

7.2 Simulation results

This section demonstrates the results and observations of the proposed SPAWN. The proposed SPAWN is compared with MIPMANET and AODV under the same network settings with respect to the metrics of packet delivery ratio, end-to-end delay, routing packet overhead and throughput.

Figure 6a shows the performance of SPAWN under node mobility such as 0, 2, 4 m/s, etc. The packet delivery ratio of SPAWN is better than MIPMANET and far better than AODV with varying mobile speed. The packet delivery ratio is 98% for SPAWN and MIPMANET when there is no mobility whereas it is 89% for AODV. Under the mobility of 10 m/s the SPAWN provides 92% of packet delivery ratio which is better than MIPMANET and AODV. Figure 6b shows the end-to-end delay of all the three protocols. The proposed SPAWN shows the minimal delay than the rest of the protocols. Figure 6c demonstrates the routing packet

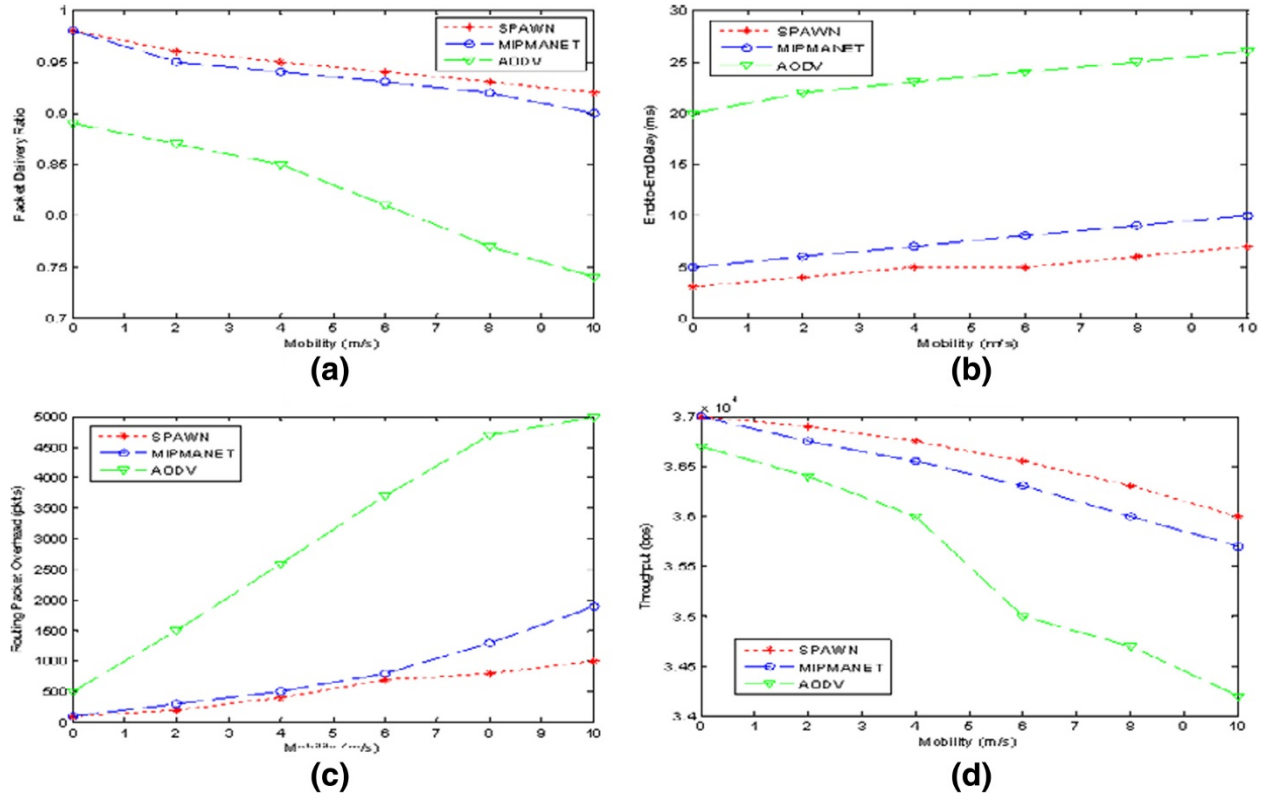

Figure 6 Performance comparison of SPAWN, MIPMANET and AODV under mobility. **(a)** Mobility vs. packet delivery ratio. **(b)** Mobility vs. end-to-end delay. **(c)** Mobility routing packet overhead. **(d)** Mobility vs. throughput.

overhead of SPAWN and MIPMANET that is almost similar under the mobility of up to 6 m/s but there is a significant difference for both the protocols under the mobility of 10 m/s. The AODV has got the high overhead than SPAWN and MIPMANET. Figure 6d shows that when there is no mobility, the throughput of SPAWN and MIPMANET is equal but for AODV, it is less. But under varying speed of mobile nodes, the SPAWN performs better than rest of the two protocols.

Obviously, as the number of misbehaving nodes increases in the network, the number of genuine/trusted nodes decreases. Thus, decreases the routing performance. The proposed SPAWN is compared with MIPMANET and AODV with varying number of misbehaving nodes. Figure 7a shows that the packet delivery ratio is almost similar for all the three protocols but the performance going down when the misbehaving nodes increases gradually. When 50% of the mobile nodes are misbehaving in the network, the packet delivery ratio of SPAWN is 82% whereas it is 80% and 50% for MIPMANET and AODV, respectively. Figure 7b shows that the end-to-end delay of the proposed SPAWN performs significantly better than MIPMANET and AODV when the misbehaving nodes increase from 0% to 50%. In Figure 7c, the routing packet overhead of SPAWN is very close to MIPMANET but far better than AODV. Figure 7d shows that comparatively, SPAWN has got better throughput than both the MIPMANET and AODV with varying number of misbehaving nodes.

8. Conclusions

The SPAWN addresses the privacy and security issues in mobile ad hoc networks when it is integrated with the fixed network to access the internet. The architecture adapts the modules such as watchdog, trust estimation and reputation in order to monitor and determine the mobile nodes trust and reputation. Based on these factors, an observer decides the node state and reports to the other users in the network if it is a misbehaving node (outlier or malicious). The SPAWN adapts the k-times anonymous authentication scheme and onion routing to achieve privacy- and security-related goals. So, the proposed architecture has its own importance in mobile ad hoc networks in the integrated environment. The simulation results prove the performance of SPAWN.

The proposed architecture is suitable for a constrained number of mobile nodes. If the number of mobile nodes exceeds the threshold in a network, then the mobile

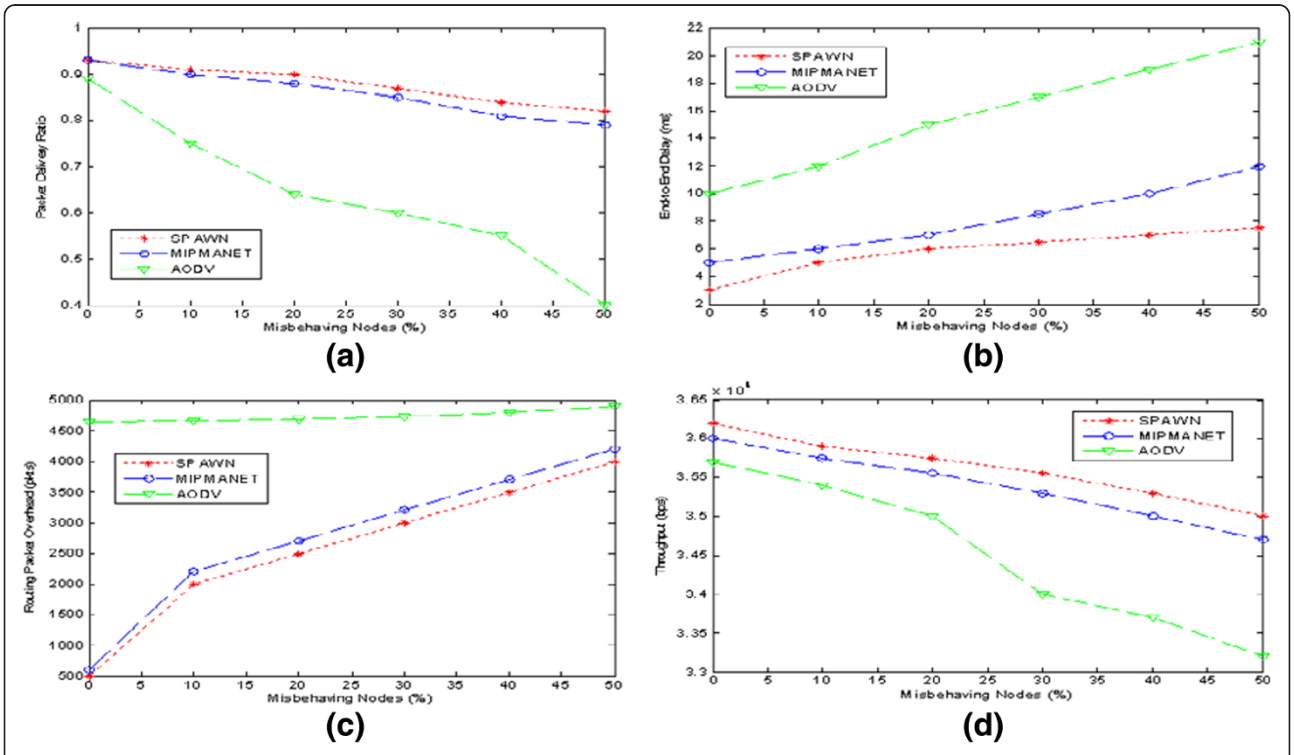

Figure 7 Performance comparison of SPAWN, MIPMANET and AODV with varying number of misbehaving nodes. (a) Misbehaving nodes vs. packet delivery ratio. **(b)** Misbehaving nodes vs. end-to-end delay. **(c)** Misbehaving nodes vs. routing packet overhead. **(d)** Misbehaving nodes vs. throughput.

node energy consumption is comparatively high. So, the scalability factor needs to be considered in addition with existing concepts in the future.

Competing interests
The authors declare that they have no competing interests.

Received: 1 March 2013 Accepted: 14 August 2013
Published: 4 September 2013

References

1. J Qaddour, R Barbour, *Evolution to 4G wireless: problems, solutions, and challenges* (Paper presented in the 3rd ACS/IEEE international conference on computer systems and applications, Cairo, Egypt, 2005), pp. 78–I
2. D Axiotis, T Al-Gizawi, K Peppas, E Protonotarios, F Lazarakis, C Papadias, P Philippopoulos, Services in interworking 3G and WLAN environments. IEEE Wirel Commun. **11**(5), 14–20 (2004)
3. M Lott, M Siebert, S Bonjour, D von Hugo, M Weckerle, Interworking of WLAN and 3G systems. IEE Proc Comm. **151**(5), 507–513 (2004)
4. N Komninos, DD Vergados, C Douligeris, A two-step authentication framework for mobile ad hoc networks. China Commun J. **4**(1), 28–39 (2007)
5. K El Defrawy, G Tsudik, Privacy-preserving location-based on-demand routing in MANETs. IEEE J Sel Area Comm. **29**(10), 1926–1934 (2011)
6. A Loay, K Ashfaq, G Mohsen, A survey of secure mobile ad hoc routing protocols. IEEE Commun Surv Tutorials. **10**(4), 78–93 (2008)
7. P Jianli, P Subharthi, J Raj, A survey of the research on future internet architectures. IEEE Commun Mag. **49**(7), 26–36 (2011)
8. FM Abduljalil, SK Bodhe, A survey of integrating IP mobility protocols and mobile ad hoc networks. IEEE Commun Surv Tutorials. **9**(1), 14–30 (2007)
9. A Irshad, M Shafiq, A Rahman, S Khurram, M Usman, E Irshad, A secure interaction among nodes from different MANET groups using 4G technologies, in *International Conference on Emerging Technologies* (Islamabad, 2009), pp. 476–481
10. D Shuo, A Survey on Integrating MANETs with the Internet: Challenges and Designs. Comput Comm. **31**(14), 3537–3551 (2008)
11. C Imrich, C Marco, L Jennifer, Mobile ad hoc networking: imperatives and challenges. Ad Hoc Netw. **1**(1), 13–64 (2003)
12. Y Sun, E Royer, CE Perkins, Internet connectivity for ad hoc mobile networks. Int J Wireless Inform Network. **9**(2), 75–78 (2002)
13. I Teranishi, J Furukawa, K Sako, K-times anonymous authentication, in *Proceedings of ASIACRYPT* (Jeju Island, 2004), pp. 308–322
14. J Kong, X Hong, ANODR: Anonymous On-Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks, in *Proceedings of 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (Annapolis, 2003), pp. 291–302
15. R Wakikawa, H Matsutani, R Koodli, A Nilsson, J Murai, Mobile Gateways for Mobile Ad-Hoc Networks with Network Mobility Support, in *Proceedings of 4th International Conference on Networking* (Reunion Island, France, 2005), pp. 17–21
16. U Jonsson, F Alriksson, T Larsson, P Johansson, J Maguire, *MIPMANET Mobile IP for Mobile Ad Hoc Networks* (Paper presented in the 1st annual workshop on mobile and ad hoc networking and computing, Boston, MA, 2000), pp. 75–85
17. J Broch, DA Maltz, DB Johnson, Supporting Hierarchy and Heterogeneous Interfaces in Multi-hop Wireless Ad Hoc Networks, in *Proceedings of the International Symposium on Parallel Architectures, Algorithms and Networks* (Perth, 1999), pp. 370–375
18. BA Kock, JR Schmidt, *Dynamic Mobile IP Routers in Ad Hoc Networks* (Paper presented in the international workshop on wireless ad-hoc networks, Netherlands, 2004), pp. 130–134
19. Y Tseng, C Shen, W Chen, Integrating mobile IP with ad hoc networks. IEEE Comput Soc. **36**(5), 48–55 (2003)
20. J CE Perkins, NY Thomas, Yorktown Heights, Mobile-IP, Ad-hoc Networking, and Nomadicity, in *Proceedings of 20th International Conference on Computer Software and Applications Conference* (Seoul, 1996), pp. 472–476
21. MG Reed, PF Syverson, DM Goldschlag, Anonymous connections and onion routing. IEEE J Sel Area Comm. **16**(4), 482–494 (1998)
22. S Seys, B Preneel, ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks, in *Proceedings of the International Conference on Advanced Information Networking and Applications* (IEEE Computer Society, Washington, DC, Switzerland, 2009), pp. 145–155
23. D Sy, R Chen, L Bao, ODAR: On-Demand Anonymous Routing in Ad Hoc Networks, in *Proceedings of the 3rd IEEE International Conference on Mobile Ad-hoc and Sensor Systems* (Vancouver, BC, 2006), pp. 267–275
24. Y Zhang, W Liu, W Lou, Y Fang, MASK: anonymous on-demand routing in mobile ad hoc networks. IEEE Trans Wireless Comm. **5**(9), 2376–2385 (2006)
25. H Choi, W Enck, J Shin, P McDaniel, T La Porta, ASR: anonymous and secure reporting of traffic forwarding activity in mobile ad hoc networks, Springer Link. Wireless Netw. **15**(4), 525–539 (2009)
26. B Zhu, K Ren, L Wang, Anonymous Misbehavior Detection in Mobile Ad Hoc Networks, in *Proceedings of 28th International Conference on Distributed Computing Systems Workshops* (IEEE Computer Society, Beijing, 2008), pp. 358–363
27. J Pan, J Li, MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Networks, in *Proceedings of the International Conference on Management and Service Science* (Wuhan, 2009), pp. 1–6
28. H Cha, J Park, H Kim, *Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks, Internet-Draft draft-cha-manet-extended-support-globalv6-00.txt* (Mobile Ad Hoc Networking Group, South Korea, 2003)
29. J Xi, C Bettstetter, Wireless Multi-Hop Internet Access: Gateway Discovery, Routing, and Addressing, in *Proceedings of International Conference on Third Generation Wireless and Beyond (3Gwireless)* (San Francisco, 2002)
30. C Perkins, E Belding-Royer, S Das, *Ad Hoc On-Demand Distance Vector (AODV) routing, RFC 3561*, 2003
31. M Gunasekaran, K Premalatha, TEAP: trusted-enhanced anonymous on demand routing protocol for mobile ad hoc networks. IET Inf Secur. **7**(3), 203–211 (2012)
32. D Johnson, A Menezes, S Vanstone, The elliptic curve digital signature algorithm (ECDSA). Int J Inform Secur. **1**(1), 36–63 (2001)
33. Q Huang, D Jao, HJ Wang, *Applications of Secure Electronic Voting to Automated privacy Preserving Troubleshooting* (ACM, New York, 2005), pp. 68–80

doi:10.1186/1687-1499-2013-220
Cite this article as: Gunasekaran and Premalatha: **SPAWN: a secure privacy-preserving architecture in wireless mobile ad hoc networks.** *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:220.