A secure routing protocol with node selfishness resistance in MANETs

Chun-Ta Li

Department of Information Management,
Tainan University of Technology,
529 Zhongzheng Road, 710 Tainan, Taiwan, R.O.C.
E-mail: th0040@mail.tut.edu.tw

Chou-Chen Yang

Department of Management Information Systems,
National Chung Hsing University,
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
E-mail: cc.yang@nchu.edu.tw

Min-Shiang Hwang*

Department of Computer Science and Information Engineering,
Asia University,
500 Lioufeng Road, 413 Taichung, Taiwan, R.O.C.
E-mail: mshwang@asia.edu.tw
*Corresponding author

Abstract: In mobile ad hoc networks (MANETs), available nodes must act as their own router and also rely on other nodes to relay communication packets. However, some intermediate nodes may refuse to forward packets to other nodes or discard route-discovery requests from others to save power, as much as those consumed during the message transmission phase. In order to prevent node selfishness, we have proposed a novel approach to message security using a payment-based mechanism in MANETs. In this way, the proposed routing protocol with payment mechanism not only avoids the selfish nodes that may refuse to route packets, but also restrains the nodes from sending useless packets into the networks. Finally, the proposed payment mechanism ensures ad hoc communications in a selfless environment by providing economic encouragement to enforce node cooperation in MANETs.

Keywords: Identity-based cryptography; Mobile ad hoc networks; Mobile communication; Routing protocol; Network security.

Reference to this paper should be made as follows: Li, C.T., Yang, C.C. and Hwang, M.S. (xxxx) 'A secure routing protocol with node selfishness resistance in MANETs', *Int. J. Mobile Communications*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Chun-Ta Li received his Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taichung, Taiwan, ROC, in 2008. He is currently an assistant professor of the Department of Information Management, Tainan University of Technology, Tainan, Taiwan, ROC. He is a member of IEEE, a member of Chinese Information Security Association. His research interests include information security, wireless sensor networks, P2P security, and security protocols for ad hoc networks. Dr. Li has published more than 30 international journal and conference papers on the above research fields.

Chou-Chen Yang is currently a full-time professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan, ROC.

Min-Shiang Hwang received his Ph.D. degree in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He is currently a chair professor of the Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 100+ articles on the above research fields in international journals.

1 Introduction

With recent advances in wireless communication and pervasive computing technologies, mobile ad hoc networks (MANETs) are increasingly being adopted for a wide variety of applications, such as military battlefield surveillance, rescue missions, civil enforcements, e-voting, and service discoveries (Al-Bahadili, Hussain, Issa, and El-Zayyat, 2011), (Bouassida, Chrisment and Festor, 2008), (Li, Hwang and Chu, 2008), (Li, Hwang and Liu, 2008), (Li and Chu, 2009), (Li, Hwang and Chu, 2009), (Merwe, Dawoud and Mcdonald, 2007), (Sieka and Kshemkalyani, 2007), (Wei, Hwang, and Chin, 2011), (Zhang, Liu, Lou and Fang, 2006). A mobile ad hoc network can be quickly deployed to designated areas while consisting of available nodes of which two nodes can directly communicate with each other wirelessly, as long as they are within wireless radio communication range, without any fixed infrastructure (Mal-Sarkar, Sikder, Yu and Konangi, 2009). Moreover, available nodes must both act as routers for themselves and also rely on other nodes to relay communication data. As a result, the communication between two nodes is usually forwarded through a number of intermediate nodes, while the transmission range of a node is assumed to be limited.

Traditional wired networks are well-protected by several lines of defense, such as firewalls and centralized administration. However, wireless ad hoc networks do lack these defenses, so security attacks may come from any direction and could target all available nodes. Various attacks have been proposed, such as passive eavesdropping, active tampering, interfering, and spamming. Therefore, in order to ensure the security of two communication nodes, a protocol must enable a destination node to identify the source of a given message, and the source node must be able to authenticate the legal destination node (Wei, Hwang, and Chin, 2011). A reliable network is essential to ensure a quality service. However, as many mobile devices such as PDAs that use MANETs do have limited power (Shin and Weiss, 2010), (Shin and Weiss, 2010), because some intermediate nodes may refuse to route packets to a destination or directly discard route-discovery requests from others to save power. Over the course of time, this type of stop forwarding attack may lead nodes in the network to be uncooperative and selfish. To overcome the above situations, we have integrated the payment-based concept into a routing protocol to encourage node cooperation in MANETs. The payment-based scheme (Buttyan and Hubaux, 2003) has the ability to promote better performances by providing economic encouragement. Most research concerned with this area have focused on two types in MANETs, namely (1) packet purse model (PPM) and (2) packet trade model (PTM). In the PPM, the source node pays for the request and the intermediate nodes all gain from it. Alternatively, in the PTM, the intermediate node buys the packet from its ancestor node and sells it to the successor node on the route. Finally, the destination node receives the message by buying the packet from its ancestor node. The PPM restrains the nodes from sending the useless packets into networks, and prevents networks from packet flooding attacks. On the contrary, PTM is vulnerable to packet flooding attacks because the malevolent nodes may send a large number of useless packets into a network to obtain the financial incentive. As a result, our proposed protocol focuses on the PPM and integrates it into a routing algorithm. Moreover, our proposed protocol maintains the following essential requirements:

- For MANETs security, it is important to provide mutual authentication, data confidentiality, and integrity between the two communicating nodes. Therefore, ad hoc nodes have to generate the dynamic session keys to secure the communications in MANETs. Moreover, participant nodes must have light overheads in terms of computational costs, and high efficiency.

- Preventing active tampering attacks, that is, no one can alter a message to damage the security of MANETs. If a malicious node on the route tampers with the packet, it can be detected and identified by running a detection of malicious intermediate nodes.

- Providing non-repudiation, that is, it not only leads to identification of the sources of received information, but also prevents a sender from denying a sent message if it has done so. As a result, the non-repudiation can prevent impersonation attacks, in other words, an intruder cannot pretend to be a legitimate node.

To the best of our knowledge, the research done in this paper is the first attempt to provide a secure communications model with mutual authentication, key establishment protocol, detection of malicious intermediate nodes, and prevention of node selfishness in mobile ad hoc networks. Since a payment-based routing protocol also requires the cryptographic encryption and verification, we used the Identity-Based Encryption (IBE) scheme (Boneh and Franklin, 2001) to reduce the overhead of verifying certificates every time. In identity-based cryptography, there is no need for users to maintain other users' public key certificates, and the publicly known identity of a user can be used to derive the public key of the user. Our protocol assumes that the network has a Key Generator Center (KGC), which is trusted by all nodes in the network. In addition, a KGC is used for generating a master key and other necessary parameters for authorized nodes to form a secure MANET environment. This will be further described in Section 2.

The rest of this article is organized as follows. We will first discuss the related works and their limitations in Section 2. In Section 3 we will present a secure routing protocol with payment mechanism. In Section 4, security analysis is presented; followed by our conclusions in Section 5.

2 Related works

To ensure safety, routing is a critical issue in MANETS because of its special characteristics and a number of secure routing protocols have been proposed (Hassan, El-Aziz, and El-Radi, 2010), (Hsu and Chang, 2009), (Hu, Perrig and Johnson, 2002), (Li, Hwang and Chu, 2008), (Papadimitratos and Haas, 2002), (Papadimitratos and Haas, 2003), (Park, Song, Lee, Kim, Lee and Moon, 2007), (Xia and Wang, 2006) for MANETs, such as SRP (Papadimitratos and Haas, 2002), SEAD (Hu, Perrig and Johnson, 2002), SMT (Papadimitratos and Haas, 2003), DIMH (Xia and Wang, 2006), SRDP (Park, Song, Lee, Kim, Lee and Moon, 2007), SDMP (Othman and Mokdad, 2010), and RSSRE (Yu, Guo, Wang and Liu, 2009). They are generally classified into two categories: reactive and proactive protocols. In reactive protocols (also called source-initiated on-demand driven protocols), routing data does not need to be periodically maintained and related routing data is initiated whenever the packets are required to be sent. On the other hand, in proactive protocols (also called table-driven protocols), participating nodes are required to periodically maintain and update routing data and to store it in their own routing tables, even if no packets are required to be sent. These protocols are integrated with some protective mechanisms for enhancing the confidentiality of transmitted messages between two communication nodes such as message encryption, node authentication, multipath routing, reputation/trust evaluation and anonymous routing.

For QoS routing, it requires not only to find a path from the source node to the destination node, but a path that satisfies the end to stop QoS bandwidth/delay/packet loss requirements for real-time applications (such as audio, video, etc.). The work developed in (Du, 2004) draws up the issue of a MANET wishing to provide a maximum available bandwidth in a given path, while having a lower packet delay and a higher throughput than AODV (Perkins and Royer, 1999). The idea in (Wu and Jia, 2007) is based on the concept of multiple paths, or multiple trees, to meet the bandwidth requirement of a call. Each node maintains its local routing information without maintaining the global information of the network topology, and thus the network resources can be better utilized.

The reputation/trust mechanism is built based on ad hoc nodes that have shown benign behaviors will get a better service from their peers by awarding a better reputation or trust. The work (Narula, Dhurandher, Misra and Woungang, 2008) proposes a novel method of message security by using the trust levels into multipath routing algorithm to avoid non-trusted routes that may use brute force attacks. The authors in (Yu, Guo, Wang and Liu, 2009), that present a reputation-based routing scheme for hierarchical ad hoc networks and the cluster head, act as the reputation manager for updating reputation information with different roles. Thus, the malicious nodes would be isolated for safeguard routing security.

In order to stimulate the nodes for packet forwarding, authors in (Buttyan and Hubaux, 2003) assume that every node has a tamper resistant security module (such as a smart card) and the security module maintains a counter, called *nuglet counter*. The *nuglet counter* is increased by one when the intermediate node forwards a packets for the benefit of other nodes and the *nuglet counter* is decreased by n when the source node wants to send its own packets, where n is the number of intermediate nodes needed to reach the destination and *nuglet counter* required to remain always positive. However, all the routing packets between the involved participants are protected by the session key and thus the security requirement of data non-repudiation cannot be provided. The integrity of a received packets can be verified only by an intermediate node and the intermediate node cannot prove the source of the received packets to any third party. Without guarantee the validity of sender's transmission behavior, a source node may deny its forwarding requests.

3 A secure routing protocol with payment mechanism

In this section, we proposed our secure routing protocol with substantial payment for MANETs. It is aimed to prevent active attacks, such as stop forwarding and tampering attacks in which malicious nodes could alter packets in transit and damage network communication. Before presenting the details of our payment-based routing protocol, we must outline some basic notations and assumptions, as seen in Tables 1 and 2, respectively. The whole protocol consists of three phases: a path discovery phase, a path reverse phase, and a data transfer phase with payment mechanism. In general, a routing protocol consists of three types of participants: source node N_0, destination node N_n, and intermediate nodes N_i, where $i = 1, 2, \ldots, n-1$. The source node initiates a path discovery phase from itself to the destination node by sending a *PathDiscovery* message through a number of intermediate nodes. Then, the destination node responds with a *PathReverse* message in the reverse direction until it reaches the source node, verifying the complete route. For the data transfer phase, N_0 sends a confidential message M to N_n through a number of intermediate nodes, and the involved intermediate nodes along the route may demand to be paid for forwarding packets to the successor node until M reaches N_n. As a result, N_0 will generate $n-1$ pieces of $Nuglet$ and pay them for the involved intermediate nodes, where $Nuglet$ is the virtual currency. In addition, all messages transmitted between nodes should be verified and protected in the protocol. Thus even if adversaries could eavesdrop on the communications between nodes, or inject false packets into networks, the

Table 1 Notations

Notation	Description
ID_i	The identity of node i.
N_0	The source node.
N_n	The destination node.
N_i	The intermediate nodes, where $i = 1, 2, \cdots, n-1$.
(Q_{ID_i}, S_{ID_i})	A public key and private key of node i, where $Q_{ID_i} = H_1(ID_i) \in \mathbb{G}_1^*, S_{ID_i} = sQ_{ID_i}$, and s is the master key.
tag#	An unique tag number for a route.
$\triangle$	A notation for a field in a local route table, which records when the value of this field is temporarily unknown.
SK_i^j	A static shared key between node N_i and node N_j, where $SK_i^j = Q_{ID_j} \times S_{ID_i} = Q_{ID_j} \times s \times Q_{ID_i} = Q_{ID_i} \times S_{ID_j} = SK_j^i$.
$H_1(.)$	A cryptographic hash function, where H_1:{0,1}*$\to \mathbb{G}_1^*$.
$H_2(.)$	A public and collision-free hash function, where $H_2 : \mathbb{G}_2 \to \{0,1\}^n$.
MAC	The message authentication code and is defined by $MAC = H_2(k; M)$, where m denotes the message under the protection key of k.
$Nuglet_{i,j}$	A virtual currency which is generated by node i and node i paid $Nuglet_{i,j}$ to node j for the services.
hop	The number of hops that a message can transmit.
$a\|\|b$	Concatenation of message a and b.
$E_{SK}[.]$	The symmetric encryption function with shared session key SK.
$D_{SK}[.]$	The symmetric decryption function with shared session key SK.
$E_{Q_{ID_i}}\{.\}$	The asymmetric encryption function with node i's public key Q_{ID_i}.
$D_{S_{ID_i}}\{.\}$	The asymmetric decryption function with node i's private key S_{ID_i}.

protocol would provide an adequate level of security. In the following subsection, each phase is described in detail.

3.1 Path discovery phase

Initially, whenever a source node N_0 attempts to securely establish an available route path from itself to the destination node N_n, it would first generate a unique tag#, and then initiates a path discovery procedure within the network to find a feasible route by performing the following operations, as depicted in Figure 1.

(1) Computes $X = xP$ and sets a suitable number of hops to be *hop*, where P is a generator of $\mathbb{G}_1$, $\mathbb{G}_1$ is an additive group of prime order q, x is a random number. Note that *hop* is depending on the actual frequency of usage.

(2) Chooses a random value m and computes the list of values $h_0, h_1, h_2, \cdots$, h_{m-1}, h_m, where $h_0 = m$ and $h_i = H_2(h_{i-1})$, for $0 < i \leq m$.

Table 2 Assumptions

A-1	The links between connected mobile nodes are bi-directional, also the mapping between the node i identifier ID_i and its corresponding public key is clear to every node that participates in the ad hoc network.
A-2	Each node is capable of executing $E_{pk_i}\{.\}$, $D_{sk_i}\{.\}$, $E_{SK}[.]$, $D_{SK}[.]$, and $H(.)$ algorithms.
A-3	The static shared key SK_i^j is protected by node U_i and node U_j, and the node would never shares its private key with anyone else.
A-4	An attacker may un-intrusively eavesdrop, modify, or re-send messages into the wireless channel between two communication nodes in MANETs. However, we assumed that the proposed protocol does not provide a mechanism against a Denial-of-Sevice (DOS) attack. For this type of attack, an attacker can simply disrupt, subvert, or destroy a network. Note that this kind of attack is common throughout all protocols in MANETs.
A-5	A Key Generator Center (KGC) is used to generate a master key s, and the master key is kept secretly by the KGC. Moreover, KGC must publish some system parameters and privately send each node the corresponding private key along with its public key.
A-6	Node i maintains its local route table (LRT_i) for a special route, and the format of LRT_i is shown as follows. $(tag\#, Ancestor, Succesor, Hash\_chain\_value, Life-time)$ where the 1st field of LRT_i means the unique tag number for a route, the 2nd field records its ancestor node, the 3th field records its successor node, the 4th field records the hash chain value which is generated by the source node, and the 5th field indicates a life-time which controls how long a route is valid in LRT_i. If the value of life-time hits 0, the entry will be removed from LRT_i.

Path discovery phase		
N_0		N_1
(1) Compute $X = xP$		(6) Check if $((hop--) \geq 0)$
(2) Compute $h_i = H_2(h_{i-1})$, for $0 < i \leq m$		(7) Check $tag\#$
(3) Make $MPD_{N_0} = \{N_0 \| \| N_n \| \| X \| \| h_m \| \| h_{N_0}\}$		(8a) $LRT_1 =$
(4) Broadcast $packet = [tag\# \| \| hop \| \| MPD_{N_0}]$		$(tag\#, N_0, \triangle, h_m, LT_{N_1})$
(5) $LRT_0 = (tag\#, N_n, \triangle, h_m, LT_{N_0})$	$\xrightarrow{packet}$	
N_i		N_{i+1} $(1 \leq i \leq n-1)$
(8a) $packet = [tag\# \| \| hop \| \| MPD_{N_i}]$		
$LRT_i = (tag\#, N_n, \triangle, h_m, LT_{N_i})$	$\xrightarrow{packet}$	
N_{n-1}		N_n
(8a) $packet = [tag\# \| \| hop \| \| MPD_{N_{n-1}}]$		(8b) Verify h_{N_i}
$LRT_{n-1} = (tag\#, N_{n-2}, \triangle, h_m, LT_{N_{n-1}})$		$LRT_n =$
	$\xrightarrow{packet}$	$(tag\#, N_{n-1}, N_0, h_m, LT_{N_n})$

Figure 1 Path discovery phase

(3) Makes a *PathDiscovery* message MPD_{N_0} as $MPD_{N_0} = \{N_0 \ ||N_n \ ||X \ ||h_m \ ||h_{N_0}\}$, where $h_{N_0} = H_2(tag\#||N_0||N_n||X||h_m||SK_{N_0}^{N_n})$ and $SK_{N_0}^{N_n} = Q_{ID_{N_n}} \times S_{ID_{N_0}} = Q_{ID_{N_n}} \times s \times Q_{ID_{N_0}} = Q_{ID_{N_0}} \times S_{ID_{N_n}} = SK_{N_n}^{N_0}$.

(4) Broadcasts a *PathDiscovery* packet to the neighbors within the wireless transmission range, where $packet = [tag\#||hop||MPD_{N_0}]$.

(5) Stores the entry $(tag\#, N_n, \triangle, h_m, LT_{N_0})$ in its local route table LRT_0. Since N_0 itself is the source of this route and no ancestor node exists, the second field records the identity of N_n. Also, the third field is temporarily unknown at this point, and it would be added later during the path reverse phase. The fourth field records the hash chain value h_m, and this field is used for nodes N_i to verify the legitimacy of a received message, where $i = 1, 2, \ldots, n$. The fifth field records the life-time of an entry on the route. The entry would be deleted if the timer hits to 0.

When a node receives the *PathDiscovery* packet, it will perform the following steps:

(6) Check if $((hop--) \geq 0)$, if it holds, continue; otherwise, stop.

(7) Check if the *PathDiscovery* packet has already been received from other nodes within its wireless transmission range while using the unique tag# as the unique identifier for this route. If it holds, drop it and stop; otherwise, continue.

(8) Check if the node itself is the designated receiver. There are two possible outcomes:

a. If the node is NOT the designated receiver, then it maintains its local route table LRT$_i$=(tag#,$N_{i-1}, \triangle, h_m, LT_{N_i}$) and computes $h_{N_i} = H_2(N_i||h_{N_{i-1}})$. Then, N_i appends its identity to the route list RL and forwards the new packet (tag#$||hop--||MPD_{N_i}$) to the neighboring nodes, where $0 < i \leq n-1$ and $MPD_{N_i} = \{N_0 \; ||N_n \; ||X \; ||h_m \; ||h_{N_i} \; ||RL = (ID_{N_1}, ID_{N_2}, \ldots, ID_{N_{i-1}}, ID_{N_i})\}$.

b. If the node is the intended destination for node N_n, it computes $h_{N_n} = H_2(tag\#||N_0||N_n||X||h_m||SK_{N_n}^{N_0})$ and the list of values $h_{N_1}, h_{N_2}, \cdots, h_i$, where $SK_{N_n}^{N_0} = Q_{ID_{N_0}} \times S_{ID_{N_n}} = Q_{ID_{N_0}} \times s \times Q_{ID_{N_n}} = Q_{ID_{N_n}} \times S_{ID_{N_0}} = SK_{N_0}^{N_n}$, $h_{N_1} = H_2(N_1||h_{N_n})$ and $h_{N_i} = H_2(N_i||h_{N_{i-1}})$, for $0 < i \leq n-1$. Then, N_n checks whether the hash chain h_{N_i} is correct. If the hash chain value is satisfied, the *PathDiscovery* message is deemed valid. Finally, N_n stores the following entry ($tag\#$, N_{n-1}, N_0, h_m, LT_{N_n}) in its local route table LRT_n. Since N_n itself is the destination of this route and has no successor node, the third field records the identity of N_0. The second field then records its ancestor node N_{n-1}, and the fourth field records the hash chain value h_m. The fifth field records the life-time LT_{N_n} of an entry in the route. Upon the entry of all necessary records, the path discovery phase ends.

3.2 Path reverse phase

Figure 2 illustrates the path reverse phase of our proposed payment-based routing protocol. To initiate a path reverse session, the destination node N_n first initiates a path reverse procedure in the reverse direction to confirm a complete route from itself to the source node N_0 by performing the following operations.

(1) Computes $Y = yP$ and $DSK_{N_n}^{N_0} = y \times X = xyP$, where y is a random number and $DSK_{N_n}^{N_0}$ is a dynamic session key between N_n and N_0.

(2) Makes a *PathReverse* message MPR_{N_n} as $MPR_{N_n} = \{N_n \; ||N_0 \; ||Y \; ||h_m \; ||MAC_{N_n}\}$, where $MAC_{N_n} = H_2(DSK_{N_n}^{N_0}; tag\#||N_n||N_0||Y||RL||h_m||SK_{N_n}^{N_0})$.

(3) Unicasts a *PathReverse* packet as $packet = [tag\#||RL||MPR_{N_n}||Sig_{N_n} = E_{S_{ID_{N_n}}}\{MAC_{N_n}\}]$ to its ancestor node N_{n-1}, where $RL = (ID_{N_0}, ID_{N_1}, \ldots, ID_{N_{n-1}}, ID_{N_n})$ and $E_{S_{ID_{N_i}}}\{*\}$ stands for signing $\{*\}$ with the private key of node N_i.

Upon receiving the *PathReverse* packet from N_n, N_{n-1} deals with this packet according to following steps.

(4) Checks whether $tag\#$ exists in LRT_{n-1} or not. If a tag is found, continue; otherwise, stop.

Path reverse phase		
N_{n-1}		N_n
		(1) Compute Y and $DSK_{N_n}^{N_0}$
		(2) Make $MPR_{N_n} = \{N_n \| N_0 \| Y \| h_m \|$ $MAC_{N_n}\}$
(4) Check $tag\#$		
(5) Verify $MAC_{N_n} = D_{Q_{ID_{N_n}}}\{Sig_{N_n}\}$		(3) Unicast $packet = [tag\# \| RL \|$ $MPR_{N_n} \| Sig_{N_n}]$
(6) Compute $Sig_{N_{n-1}}$	$\xleftarrow{packet}$	
(7) Unicast $packet = [tag\# \| RL \|$ $MPR_{N_n} \| Sig_{N_{n-1}}]$		
(8) $LRT_{n-1} = (tag\#, N_{n-2}, N_n, h_m, LT_{N_{n-1}})$		
N_{i-1}		$N_i (1 \leq i \leq n-1)$
		(4) Check $tag\#$ (5) Verify $Sig_{N_{i+1}}$
		(6) Compute Sig_{N_i}
		(7) Unicast $packet = [tag\# \| RL \|$ $MPR_{N_n} \| Sig_{N_i}]$
	$\xleftarrow{packet}$	(8)$LRT_i = (tag\#, N_{i-1}, N_{i+1}, h_m, LT_{N_i})$
N_0		N_1
		(4) Check $tag\#$ (5) Verify Sig_{N_2}
(9) Verify Sig_{N_1}		
(10) Compute $DSK_{N_0}^{N_n}$		(6) Compute Sig_{N_1}
Verify $MAC_{N_n} = H_2(DSK_{N_0}^{N_n};$ $tag\# \| N_n \| N_0 \| Y \| RL \| h_m \| SK_{N_0}^{N_n})$		(7) Unicast $packet = [tag\# \| RL \|$ $MPR_{N_n} \| Sig_{N_1}]$
(11) $LRT_0 = (tag\#, N_n, N_1, h_m, LT_{N_0})$	$\xleftarrow{packet}$	(8) $LRT_1 = (tag\#, N_0, N_2, h_m, LT_{N_1})$

Figure 2 Path reverse phase

(5) Verifies if $MAC_{N_n} = D_{Q_{ID_{N_n}}}\{Sig_{N_n}\}$, if it holds, continue; otherwise, stop.

(6) Computes $Sig_{N_{n-1}} = E_{S_{ID_{N_{n-1}}}}\{H_2(ID_{N_{n-1}}||MAC_{N_n})\}$.

(7) According to the second field of LRT_{n-1}, N_{n-1} unicasts the packet to its ancestor node N_{n-2}, where $packet = [tag\#||RL||MPR_{N_n}||Sig_{N_{n-1}}]$.

(8) Maintains its local route table LRT_{n-1} as $LRT_{n-1} = (tag\#,\ N_{n-2},\ N_n,\ h_m,\ LT_{n-1})$.

Other intermediate nodes N_i along the route will perform the same steps as the node N_{n-1}, where $i = 1, 2, \ldots, n-3, n-2$. As a result, the last intermediate node N_1 should unicast $packet = [tag\#||RL||MPR_{N_n}||Sig_{N_1}]$ to its ancestor node N_0 and maintains its local route table LRT_1 as $LRT_1 = (tag\#, N_0, N_2, h_m, LT_1)$, where $Sig_{N_1} = E_{S_{ID_{N_1}}}\{H_2(ID_{N_1}||MAC_{N_n})\}$. Finally, when the source node N_0 receives the packet from N_1, it performs the following operations.

(9) Verifies if $H_2(ID_{N_1}||MAC_{N_n}) = D_{Q_{ID_{N_1}}}\{Sig_{N_1}\}$, if it holds, continue; otherwise, stop.

(10) Computes the common session key $DSK_{N_0}^{N_n}$ by computing $DSK_{N_0}^{N_n} = x \times Y = xyP = DSK_{N_n}^{N_0}$ and verifies the validity of $DSK_{N_0}^{N_n}$ by comparing with $MAC_{N_n} = H_2(DSK_{N_0}^{N_n}; tag\#||N_n||N_0||Y||RL||h_m||SK_{N_0}^{N_n})$. If it holds, not only the hash chain value h_m and the route from N_0 to N_n would be confirmed, but the dynamic session key $DSK_{N_0}^{N_n}$ as well, which is shared between N_0 and N_n, would be established by them and used to secure communications during the following data transfer phase.

(11) Maintains its local route table LRT_0 as $LRT_0 = (tag\#, N_n, N_1, h_m, LT_{N_0})$, after this path reverse phase ends.

3.3 Data transfer phase with payment mechanism

During the data transfer phase, the source node N_0 pays the virtual currency called $Nuglets$ to the involved intermediate nodes N_i alone the path, which is established during previous path's construction phases, where $i = 1, 2, \ldots, n-1$. As a result, N_0 generates $n-1$ pieces of $Nuglets_{N_0,N_i}$ as $Nuglets_{N_0,N_i} = E_{S_{ID_{N_0}}}\{tag\#, h_{m-j}, ID_{N_0}, ID_{N_i}\}$, where j denotes the transmission rounds, for $0 < j \leq m$. In addition, N_0 composes a *Payment* message that contains the complete $Nuglets_{N_0,N_i}$, the encrypted message C, and the message authentication code MAC_{N_0}. Before transmitting these messages, N_0 encrypts them with the public keys of all the nodes along the path to the destination node. Here, we will introduce an example to describe the detailed steps of data transfer phase with payment mechanism.

In the route presented in Figure 3, the *Payment* packet, sent by the source node N_0, contains the path $\{N_0, N_1, N_2, N_3\}$ forwarded to the destination node N_3. Suppose that N_0 wants to send a confidential message M to the destination node N_3, N_0 would first use the common session key $DSK_{N_0}^{N_3}$ to encrypt $C = E_{DSK_{N_0}^{N_3}}[tag\#||M]$ and computes $MAC_{N_0} = H_2(h_{m-1}; C)$, where

N_0	$\xrightarrow{MP_1, Sig_{N_0}}$	N_1	$\xrightarrow{MP_2, Sig_{N_1}}$	N_2	$\xrightarrow{C, MAC_{N_0}, h_{m-1}, Sig_{N_2}}$	N_3
		Get $Nuglets_{N_0,N_1}$		Get $Nuglets_{N_0,N_2}$		Get M

// $Nuglets_{N_0,N_1} = E_{S_{ID_{N_0}}}\{tag\#, h_{m-1}, ID_{N_0}, ID_{N_1}\}$;
// $Nuglets_{N_0,N_2} = E_{S_{ID_{N_0}}}\{tag\#, h_{m-1}, ID_{N_0}, ID_{N_2}\}$;
// $MP_1 = E_{Q_{ID_{N_1}}}\{MP_2||C||MAC_{N_0}||Nuglets_{N_0,N_1}\}$;
// $MP_2 = E_{Q_{ID_{N_2}}}\{C||MAC_{N_0}||Nuglets_{N_0,N_2}\}$;
// $Sig_{N_0} = E_{S_{ID_{N_0}}}\{C||MAC_{N_0}\}$; $Sig_{N_1} = E_{S_{ID_{N_1}}}\{C||MAC_{N_0}\}$;
// $Sig_{N_2} = E_{S_{ID_{N_2}}}\{C||MAC_{N_0}\}$; $C = E_{DSK^{N_3}_{N_0}}[tag\#||M]$; $MAC_{N_0} = H_2(h_{m-1}; C)$.

Figure 3 An example of data transfer phase with payment mechanism.

$h_m = H_2(h_{m-1})$. Then, with each encryption of the *Payment* packet, N_0 begins to compute $MP_2 = E_{Q_{ID_{N_2}}}\{C||MAC_{N_0}||Nuglets_{N_0,N_2} = E_{S_{ID_{N_0}}}\{tag\#, h_{m-1}, ID_{N_0}, ID_{N_2}\}\}$ and $MP_1 = E_{Q_{ID_{N_1}}}\{MP_2||C||MAC_{N_0}||Nuglets_{N_0,N_1} = E_{S_{ID_{N_0}}}\{tag\#, h_{m-1}, ID_{N_0}, ID_{N_1}\}\}$. Next, N_0 computes $Sig_{N_0} = E_{S_{ID_{N_0}}}\{C ||MAC_{N_0}\}$ and sends the *Payment* packet (MP_1, Sig_{N_0}) to the first intermediate node N_1. After receiving the *Payment* packet from N_0, N_1 uses its private key to remove one encryption layer to obtain the messages $Nuglets_{N_0,N_1}$, MP_2, C, and MAC_{N_0}. After obtaining them, N_1 checks Sig_{N_0} and verifies the validity of $Nuglets_{N_0,N_1}$ by comparing whether $(tag\#, h_{m-1}, ID_{N_0}, ID_{N_1}) = D_{Q_{ID_{N_0}}}\{Nuglets_{N_0,N_1}\}$ and $h_m = H_2(h_{m-1})$ are correct. If the above situation holds, it means that *Payment* packet is genuinely generated by N_0. In addition, N_1 verifies the validity of C by comparing whether $H_2(h_{m-1}; C) = MAC_{N_0}$, if it holds, continue; otherwise, stop. Next, for the purpose of non-repudiation, N_1 computes $Sig_{N_1} = E_{S_{ID_{N_1}}}\{C||MAC_{N_0}\}$ and sends *Payment* packet (MP_2, Sig_{N_1}) to the next node N_2. After receiving the packet from N_1, N_2 decrypts MP_2 using its private key $S_{ID_{N_1}}$ and verifies the validity of $Nuglets_{N_0,N_2}$, h_{m-1}, C, and Sig_{N_1}. If the above situation holds, N_2 would then compute $Sig_{N_2} = E_{S_{ID_{N_2}}}\{C||MAC_{N_0}||h_{m-1}\}$ and sends $(C, MAC_{N_0}, h_{m-1}, Sig_{N_2})$ to the destination node N_3. After receiving the packet from N_2, N_3 checks the validity of $(C||MAC_{N_0}||h_{m-1}) = D_{Q_{ID_{N_2}}}\{Sig_{N_2}\}$. If it does not hold, stop; otherwise, N_3 would check both h_{m-1} and MAC_{N_0}, and uses the common session key $DSK^{N_0}_{N_3}$ to reveal $(tag\#||M) = D_{DSK^{N_0}_{N_3}}[C]$ while checking the *tag#*. If it is correct, N_3 gets the confidential message M; otherwise, stop. Finally, N_1 and N_2 can use $Nuglets_{N_0,N_1}$ and $Nuglets_{N_0,N_2}$ to request N_0 to be paid for the services, respectively.

3.4 Detection of malicious behavior nodes

In order to ensure a secure networking, we should prevent the forged message from forwarding to the destination. The basic idea of detection of malicious behavior node is to integrate a hop-by-hop identification mechanism into routing protocol. During path reverse and data transfer phases, when a node on a path receives a packet from its previous one-hop node, it is unable to recognize whether the received packet is forged by malicious behavior node or not. However, the node can obtain the signature of the received packet from its previous node and further verify it. If the packet is valid, the node would generate the signature of received packet to its next one-hop node to guarantee the validity of its transmission behavior. Therefore, in our proposed protocol, internal attacks are detectable and the malicious nodes on a path could not deny their misbehavior if the forged message attacks were detected.

4 Security analysis

In this section, we will provide the proof that the requirements presented in Section 1 are met by our payment-based routing protocol.

Theorem 4.1: *The proposed protocol is secured against the tampering attacks and maintains data nonrepudiation of the nodes that participated in MANETs including the source node, the intermediate nodes, and the destination node.*

: During the path discovery phase, in a tampering attack, the attacker might tamper with the node list RL of $PathDiscovery$ message to facilitate further attacks, such as wormhole attacks. However, these attacks can be detected with hash chains $h_{N_i} = H_2(N_i||h_{N_{i-1}})$, for $0 < i \leq n-1$. Hash chains are used in our protocol to guarantee the correctness of transmission messages. As a result, N_n can confirm the completed route from itself to N_0 and tampering problems can be avoided in this phase.

During the path reverse phase, all the subsequent interactions between the involved participants are well-protected by the signature $Sig_{N_i} = E_{S_{ID_{N_i}}}\{H_2(ID_{N_i}\ ||MAC_{N_n})\}$, for $0 < i \leq n$. In this way, N_i ensures that the received message is indeed generated by the rightful holder of its successor node N_{i+1}. It would be apparent if an intruder does not have the rightful signature and is attempting to cheat the participants on the route to run the path reverse phases. In addition, there is no way for attackers to tamper with the node list RL of the $PathReverse$ message to wage security attacks, due to the protection of the message authentication code $MAC_{N_n} = H_2(DSK_{N_n}^{N_0}; tag\#||N_n||N_0||Y||RL||h_m ||SK_{N_n}^{N_0})$. As a result, the tampering attacks can be prevented during this phase.

Likewise, during the data transfer phase, the proposed protocol uses an approach similar to the Onion Routing protocol for transmitting the $Payment$ message MP_i, for $0 < i \leq n-1$. Thus, starting from the source node, only the corresponding intermediate node in the route can remove one encryption layer to reveal the next $Payment$ information MP_{i+1} by computing $MP_{i+1} = D_{S_{ID_{N_i}}}\{MP_i\}$. Moreover, all subsequent interactions between the participants involved are well-protected by the signature $Sig_{N_i} = E_{S_{ID_{N_i}}}\{C||MAC_{N_0}\}$, the message authentication node $MAC_{N_0} = H_2(h_{m-1}; C)$, and the hash chain value h_{m-1}; therefore this approach ensures both the security and non-repudiation during this phase. On the other hand, with respect to the security of virtual currency $Nuglets_{N_0,N_i}$, since an attacker cannot obtain the hash chain value h_{m-1} and the private key of source node, the primary requirement for such applications is payment verification, which would lead to an identification of sources of received $Nuglets_{N_0,N_i}$. As the above designed mechanism shows, the requirement of data non-repudiation and integrity can be provided in the proposed protocol. □

Theorem 4.2: *The proposed protocol maintains and ensures reliable communication for two communication nodes, and no outsiders can pretend as a legitimate node for the purpose of communicating. In other words, the impersonation attacks can be prevented in the proposed protocol.*

: During the path discovery phase, a source node N_0 sends the *PathDiscovery* message MPD_{N_0} to the destination node N_n, and the message is protected by the common shared key $SK_{N_0}^{N_n} = Q_{ID_{N_n}} \times S_{ID_{N_0}}$, which is shared only between the source node and the destination node. Thus, starting from the source node, only the destination node can derive the common shared key $SK_{N_n}^{N_0} = Q_{ID_{N_0}} \times S_{ID_{N_n}}$ to verify the validity of the message, and the security of the shared key can be provided based on ID-based public key cryptography. By expanding on $SK_{N_0}^{N_n}$ and $SK_{N_n}^{N_0}$, we have learned that $SK_{N_0}^{N_n} = Q_{ID_{N_n}} \times S_{ID_{N_0}} = Q_{ID_{N_n}} \times s \times Q_{ID_{N_0}} = Q_{ID_{N_0}} \times S_{ID_{N_n}} = SK_{N_n}^{N_0}$, if $S_{ID_{N_0}}$ is the correct private key of N_0, was issued by KGC. As a result, N_n can authenticate the validity of N_0, and vice versa. Hence, the node identification is well-protected under the proposed protocol to prevent security attacks such as impersonation attacks.

During the path reverse phase, a destination node sends the *PathReverse* message MPR_{N_n} to the source node N_0 to confirm the completed path, which is proceeded from itself to N_0 through a number of intermediate nodes N_i, for $i = 1, 2, \ldots, n-1$. The *PathReverse* message MPR_{N_n} is protected by N_n's common secret key $SK_{N_n}^{N_0}$ and dynamic session key $DSK_{N_n}^{N_0}$; while only the source node can use the corresponding private key and secret information x to derive $SK_{N_0}^{N_n}$ and $DSK_{N_0}^{N_n}$ to verify the authenticity of received messages. If the above situation holds, not only the path from N_0 to N_n would be confirmed, but also a dynamic session key $DSK_{N_0}^{N_n} = x \times Y = xyP = y \times X = DSK_{N_n}^{N_0}$ between of them will be established. Since no one has the ability to acquire and derive the static shared key between N_0 and N_n; as a result, the impersonation attacks can be resisted in MANETs in our proposed protocol. □

Theorem 4.3: *The proposed protocol is able to provide a mutual authentication and a dynamic session key between two communication nodes in a MANET. Moreover, based on the well-known Diffie-Hellman problem, SRPP also meets the security requirement for forward secrecy; even if N_0's contribution xP, and N_n's contribution yP are all known by an attacker.*

: Let X and Y be the two communication entities, namely the source node and the destination node. Let $X \overset{K_{ab}}{\longleftrightarrow} Y$ denotes the fresh session key K_{ab} shared between X and Y, and $SK_y^x = Q_{ID_x} \times S_{ID_y} = Q_{ID_y} \times S_{ID_x} = SK_x^y$ be the static shared key between node X and node Y. Hence, the mutual authentication is achieved between X and Y if there exists a session key K_{ab}, then X would believe $X \overset{K_{ab}}{\longleftrightarrow} Y$, and Y would believe $X \overset{K_{ab}}{\longleftrightarrow} Y$. As a result, we have stated that a strong mutual authentication should satisfy the following equations:

$$X \;\; believes \;\; Y \;\; believes \;\; X \overset{K_{ab}}{\longleftrightarrow} Y. \tag{1}$$

$$Y \;\; believes \;\; X \;\; believes \;\; X \overset{K_{ab}}{\longleftrightarrow} Y. \tag{2}$$

In Step (8b) of the path discovery phase, after Y receives the packet $(tag\#||hop||\ MPD_{N_{n-1}} = \{X||Y||A||h_{N_{n-1}}\})$, Y will verify $h_{N_{n-1}}$ by computing the static shared key SK_y^x, where $A = aP$, a is a random number, and P is a generator $\in \mathbb{G}_1$. Then Y could check whether the hash chain value $h_{N_{n-1}}$ is equal to $H_2(N_{n-1}||h_{N_{n-2}})$. If it holds, Y could generate a random number b and computes $B = bP$ in Step (1) of the path reverse phase. Y then computes the session key $K_{ab} = b \times A = b \times aP = abP$ and believes $X \overset{K_{ab}}{\longleftrightarrow} Y$. Also, messages B and $MAC_Y = H_2(K_{ab}; tag\#||X||Y||B||SK_y^x)$ will be sent to X.

In Step (10) of the path reverse phase, X computes the session key $K_{ab} = a \times B = a \times bp = abP$ and verifies the message MAC_Y to confirm whether this message contains (B, SK_y^x, K_{ab}). If so, X would then believe $X \overset{K_{ab}}{\longleftrightarrow} Y$. Since a is chosen by X, X believes Y and Y believes $X \overset{K_{ab}}{\longleftrightarrow} Y$.

In data transfer phase, after Y has received the encrypted message $C = E_{K_{ab}}[tag\#||M]$ from X, Y uses K_{ab} to decrypt C and check whether the message contains a response $tag\#$, where M is the confidential message. If so, Y believes $X \overset{K_{ab}}{\longleftrightarrow} Y$. Since b is chosen by Y, Y believes X and X believes $X \overset{K_{ab}}{\longleftrightarrow} Y$. Finally, after Equations (1) and (2) are satisfied, and together they accomplish the mutual authentication and dynamic session key establishment in the proposed protocol.

On the other hand, with respect to forward secrecy, we have assumed that an attacker collects X's contribution aP and Y's contribution bP during path discovery phase and path reverse phase, respectively. He/she still cannot derive the dynamic session key K_{ab}, because such process is as difficult as solving the Computational Diffie-Hellman problem (CDHP) (Barreto and Kim, 2002); and thus our proposed protocol provides perfect forward secrecy. □

5 Conclusion

In this article, a secure routing protocol with payment mechanism that prevents node selfishness for mobile ad hoc networks, is proposed. By comparison with other related schemes, the proposed protocol not only demonstrates beneficial and sought after properties (e.g., low computational costs, establishment of dynamic session keys, mutual authentication, data non-repudiation), but also provides the advantage of node cooperation encouragement. Hence, a source node can securely send a confidential message to the source node through a number of intermediate nodes while each involved intermediate node will receive a service fee *Nuglets* for his/her transmission service. Most importantly, in this way, the proposed protocol takes advantage of not only protecting a node from stop forwarding attacks by the selfish nodes, but also restrains the nodes from sending useless packets into networks and thus prevents networks from packet flooding attacks. Finally, a node could still become selfish if it has enough nuggets to transfer its own packets.

In the future research, we planned to investigate how to design a dynamic reputation algorithm into the proposed protocol regarding the issues of these nodes' behaviors. Moreover, a formal security proof and a experimental simulation would have been a better picture to demonstrate the feasibility of the proposed protocol.

References

Al-Bahadili, H., Hussain, S.M., Issa, G., and El-Zayyat, K. (2011) 'Performance evaluation of the TSS node authentication scheme in noisy MANETs', *International Journal of Network Security*, Vol. 12, pp.121–129.

Barreto, P.S.L.M. and Kim, H.Y. (2002) 'Effcient algorithms for pairing-based cryptosystems', *22nd Annual International Cryptology Cnference (Crypto'02)*, Santa Barbara, USA, pp.354–369.

Boneh, D. and Franklin, M. (2001) 'Identity-based encryption from the weil pairing', *Proceedings of Crypto 2001*, LNCS, Vol. 2139, pp.213–229.

Bouassida, M.S., Chrisment, I. and Festor, O. (2008) 'Group key management in MANETs', *International Journal of Network Security*, Vol. 6, pp.67–79.

Buttyan, L. and Hubaux, J.P. (2003) 'Stimulating cooperation in self-organizing mobile ad hoc networks', *Mobile Networks and Applications*, Vol. 8, pp.579–592.

Chang, T.Y. and Hwang, M.S. (2011) 'User-anonymous and short-term conference key distribution system via link-layer routing in mobile communications', *International Journal of Mobile Communications*, Vol. 9, pp.144–158.

Du, X. (2004) 'QoS routing based on multi-class nodes for mobile ad hoc networks', *Ad Hoc Networks*, Vol. 2, pp.241–254.

Hassan, Y.K., El-Aziz, M.H.A., and El-Radi, A.S.A. (2010) 'Performance evaluation of mobility speed over MANET routing protocols', *International Journal of Network Security*, Vol. 11, pp.128–138.

Hsu, S.C. and Chang, H.P. (2009) 'A hybrid efficient routing protocol for sink-oriented ad hoc sensor networks', *International Journal of Mobile Communications*, Vol. 7, pp.695–714.

Hu, Y.C., Perrig, A. and Johnson, D.B. (2002) 'Ariadne: a secure on-demand routing protocol for adhoc networks', *Proceedings of MOBICOM*, pp.255–265.

Li, C.T., Hwang, M.S. and Chu, Y.P. (2008) 'Improving the security of a secure anonymous routing protocol with authenticated key exchange for ad hoc networks', *Internation Journal of Computer Systems Science and Engineering*, Vol. 23, pp.227–234.

Li, C.T., Hwang, M.S. and Chu, Y.P. (2008) 'A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks', *Computer Communications*, Vol. 31, pp.2803–2814.

Li, C.T., Hwang, M.S. and Liu, C.Y. (2008) 'An electronic voting protocol with deniable authentication for mobile ad hoc networks', *Computer Communications*, Vol. 31, pp.2534–2540.

Li, C.T. and Chu, Y.P. (2009) 'Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks', *International Journal of Network Security*, Vol. 8, pp.166–168.

Li, C.T., Hwang, M.S. and Chu, Y.P. (2009) 'An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks', *International Journal of Innovative Computing, Information and Control*, Vol. 5, pp.2107-2124.

Mal-Sarkar, S., Sikder, I.U., Yu, C. and Konangi, V.K. (2009) 'Uncertainty-aware wireless sensor networks', *International Journal of Mobile Communications*, Vol. 7, pp.330–345.

Merwe, J.V.D., Dawoud, D. and Mcdonald, S. (2007) 'A survey on peer-to-peer key management for mobile ad hoc networks', *ACM Computing Surveys*, Vol. 39, pp.1–45.

Narula, P., Dhurandher, S.K., Misra, S. and Woungang, I. (2008) 'Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing', *Computer Communications*, Vol. 31, pp.760–769.

Othman, J.B. and Mokdad, L. (2010) 'Enhancing data security in ad hoc networks based on multipath routing', *Journal of Parallel and Distributed Computing*, Vol. 70, pp.309-316.

Papadimitratos, P. and Haas, Z.J. (2002) 'Secure routing for mobile ad hoc networks', *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, pp.30–38.

Papadimitratos, P. and Haas, Z.J. (2003) 'Secure message transmission in mobile ad hoc networks', *Ad Hoc Networks*, Vol. 1, pp.193–209.

Park, Y., Song, H., Lee, K., Kim, C., Lee, S. and Moon, S. (2007) 'Secure route discovery protocol for ad hoc networks', *IEICE Transactions on Fundamentals*, Vol. E90-A, pp.539–541.

Perkins, C. and Royer, E. (1999) 'Ad hoc on-demand distance vector routing', *Procedeeings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, USA, pp.90–100.

Shin, D.H. (2010) 'Ubiquitous computing acceptance model: end user concern about security, privacy and risk', *International Journal of Mobile Communications*, Vol. 8, pp.169–186.

Shin, S. and Weiss, M.B.H. (2010) 'Analysis of mobile broadband competition: 3G vs. WiFi', *International Journal of Mobile Communications*, Vol. 8, pp.586–601.

Sieka, B. and Kshemkalyani, A.D. (2007) 'Establishing authenticated channels and secure identifiers in ad-hoc networks', *International Journal of Network Security*, Vol. 5, pp.51–61.

Wei, C.H., Hwang, M.S., and Chin, A.Y.H. (2011) 'An authentication protocol for low-cost RFID tags', *International Journal of Mobile Communications*, Vol. 9, pp.208–223.

Wu, H. and Jia, X. (2007) 'QoS multicast routing by using multiple paths/trees in wireless ad hoc networks', *Ad Hoc Networks*, Vol. 5, pp.600–612.

Xia, Z. and Wang, J. (2006) 'DIMH: A novel model to detect and isolate malicious hosts for mobile ad hoc network', *Computer Standards and Interfaces*, Vol. 28, pp.660–669.

Yu, Y., Guo, L., Wang, X. and Liu, C. (2009) 'Routing security scheme based on reputation evaluation in hierarchical ad hoc networks', *Computer Networks*, Vol. 54, pp.1460–1469.

Zhang, Y., Liu, W., Lou, W. and Fang, Y. (2006) 'Securing mobile ad hoc networks with certificateless public keys', *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, pp.386–399.