A Trustworthy and Energy-Aware Routing Protocol in Software-Defined Wireless Mesh Networks

Hui Lin[1], Jia Hu[2*], Li Xu[1], YouLiang Tian[3], Lei Liu[4], Stewart Blakeway[5]

[1]*Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, 350007 China*

[2]*Department of Mathematics and Computer Science, University of Exeter, Exeter, EX4 4QF, UK*

[3]*College of Science, Guizhou University, Guiyang 550025, China*

[4]*School of Computer Science and Technology, Shandong University, Jinan 250100, China*

[5]*Department of Mathematics and Computer Science, Liverpool Hope University, L16 9JD, UK*

Abstract- Hybrid Wireless Mesh Networks (HWMNs) were proposed to address the challenges in wireless communications to support mobile applications across different domains. Due to the multi-hop and decentralized network architecture, HWMNs are naturally susceptible to various security threats, especially internal attacks. Therefore, HWMNs must be able to detect anomalies, provide secure routing and protect user privacy through the cooperation among nodes. However, the existing routing protocols for HWMNs cannot ensure the security to protect the users privacy effectively. Moreover, traditional HWMNs are vertically integrated where the control and data planes of mesh routers are bundled together, which makes it complex and difficult to configure the network according to predefined security policies, and to adaptively respond to various dynamic security threats. Software-Defined Wireless Mesh Networks decouple the control plane and data plane of routers and thus enable a more flexible and efficient configuration of security policies. Taking up this opportunity to address the aforementioned challenges, this paper proposes a privacy-aware, secure and energy-aware green routing (PSGR) protocol that can defend against internal attacks, achieve stronger privacy protection and reduce energy consumption in Software-Defined HWMNs. The elaborate theoretical analysis verify that the PSGR protocol can implement the security and privacy protection against internal attacks effectively and efficiently. Simulation results demonstrate a superior performance of PSGR in terms of packet delivery ratio, network throughput and energy efficiency compared to the existing PA-SHWMP, PASER, and HWMP protocols in the presence of Blackhole/Grayhole attacks and wormhole attacks.

Keywords- hybrid wireless mesh networks, privacy protection, energy efficiency, secure routing, software defined networks

1. INTRODUCTION

The hybrid wireless mesh networks (HWMNs) integrate both ad hoc and backbone WMNs [1, 2]. Due to the multi-hop decentralized architecture and special characteristics of the communication mode, HWMNs are exposed to various attacks, especially internal attacks launched by the internal legitimate nodes [2, 3]. As a result, HWMNs face multiple threats that could launch various internal attacks to obtain private data. Moreover, as the popularization and application scope of HWMNs expand unceasingly, more and more private information is stored in HWMNs. The leakage of such private information could bring disaster to individuals and the society. Consequently, internal attacks have become one of the most notable security problems in HWMNs [3].

As a fundamental and critical security aspect of HWMNs, the routing protocol has always been the main target of internal attacks. Various routing attacks launched from inside can damage the integrity, confidentiality and usability of private information [4]. Therefore, in order to achieve the protection of privacy and offer support for real-time applications and smooth delivery of broadband services, HWMNs must be equipped with a secure, privacy-aware and efficient routing protocol. Traditional HWMNs are vertically integrated where the control and data planes are bundled together, which makes the development and deployment of new routing algorithms very hard since it would imply a modification of the control plane of all network devices – through the installation of new firmware and, in some cases, hardware upgrades. However, Software-Defined Mesh Networks [5, 6] decouple the control plane and data plane of mesh routers, thus enable a more flexible and efficient configuration of security policies in the secure routing protocols.

The implementation of a privacy aware secure routing protocol in Software Defined HWMNs is very challenging because of the following reasons：(1) The existing HWMP routing protocols introduced in HWMNs [7,

8] are dependent on the cooperation of nodes and based on the assumption that the participating nodes are honest and well-behaved with no malicious or dishonest intentions. However, in practice nodes in a HWMN may be compromised by malicious users and are subject to various attacks from inside due to the intrinsically open and distributed nature of HWMNs [7]. (2) The mesh clients in the HWMNs could be mobile and thus are normally power constrained [8]. Therefore it is natural and imperative to consider the energy consumption of the mesh clients in routing so as to improve energy efficiency and thus prolong the battery life of the mesh clients.

To address the aforementioned issues, we propose a privacy-aware, secure and green routing protocol (PSGR) in HWMNs. In addition to achieving strong security and privacy protection, the PSGR can also maintain a good balance between security and performance. The major contributions of this work include:

(1) The proposed PSGR protocol integrates a novel dynamic reputation mechanism, a security level (SL) classified scheme and a hierarchical key management protocol in order to dynamically identify and manage the malicious nodes as well as defend against internal attacks in the routing process for HWMNs.

(2) The PSGR can further enhance privacy and security by preventing malicious nodes from modifying and interpreting packets. The energy consumption in PSGR is taken into account in the process of routing through the presented energy consumption analysis model which makes the PSGR satisfy the requirements of both security and energy-efficiency.

(3) Verified by the elaborate theoretical analyses, the PSGR protocol can implement the security and privacy protection against internal attacks effectively and efficiently. Extensive OPNET simulation experiments demonstrate that the PSGR protocol outperforms the existing routing protocols in terms of packet delivery ratio, network throughput and energy efficiency in the presence of Blackhole/Grayhole attacks and wormhole attacks.

The rest of the paper is organized as follows Section 2 presents a brief review of the related work; Section 3 describes the security, adversary and energy models; Section 4 and 5 respectively present the dynamic reputation

mechanism and the hierarchical key management protocol; Section 6 details the implementation of PSGR; Section 7 discusses the security and the analysis performance of PSGR. Finally in Section 8 concluding remarks are drawn.

2. RELATED WORK

The multi-hop decentralized architecture of HWMNs makes it difficult to design a privacy aware secure routing protocol. The early studies were devoted to applying ad hoc routing protocols for WMNs. However, due to the significant differences in the characteristics between ad hoc networks and WMNs such efforts were not fruitful [9].

Afterwards, tremendous research has focused on specific secure routing protocols in the backbone WMNs with the aim of applying them in HWMNs later on. Several cross-layer secure routing protocols with the combination of routing performance and security were proposed in [7, 10] for the backbone WMNs. These protocols combine in a cross-layered approach the different parameters from various layers across the protocol suite. For example routing-layer observations of forwarding behaviour and MAC layer to measure the quality of the wireless link in order to select the most reliable path with the highest performance. However, these routing protocols are not suitable for HWMNs due to the ad hoc nature of nodes and their ineffective privacy protection in HWMNs. Khan et al. [7] proposed the Secure Routing Protocol SRPM which is an improved AODV protocol for a backbone WMN. However, SRPM is vulnerable to the attacks launched by legitimate internal mesh nodes and thus cannot provide privacy protection effectively. Islam et al. [11] proposed a secure hybrid wireless mesh protocol (SHWMP) which is a secure extension of HWMP. However, SHWMP is also vulnerable to the attacks launched by legitimate internal mesh routers; an active attacker can compromise and control mesh routers to obtain private user information.

The infrastructure of HWMNs is highly adaptable as opposed to other networks such as the Internet, Wi-Fi, WiMAX, cellular networks or sensor networks. HWMNs are thus considered to be the most applicable architecture for future wireless communications. To make HWMNs function successfully it is imperative to design a routing protocol with security and privacy protection specifically for HWMNs. However, the secure routing protocols for

backbone WMNs are not well suited for HWMNs, thus a variety of approaches have been recently proposed for designing secure routing protocols for HWMNs. For instance, Ren et al. [12] proposed PEACE, a novel privacy-enhanced yet accountable security framework for HWMNs. However, PEACE only secures the network from external attacks and takes for granted that every internal node is cooperative and trustworthy. In [13], Khan et al. presented a cross-layer secure and resource-aware on demand routing protocol (CSROR). Because the security mechanism of CSROR is taken from the SRPM [7], it is vulnerable to the attacks launched by legitimate internal mesh nodes and cannot provide efficient privacy protection.

The existing routing protocols for HWMNs cannot ensure security or protect user privacy effectively because they are vulnerable to internal attacks. Moreover, few of the existing works have taken the energy consumption into account when making a routing decision. To bridge this gap we propose a privacy-aware, secure and green routing protocol (PSGR) in this paper. The PSGR can defend against the internal attacks effectively and achieve stronger security, privacy protection and also maintains a good balance between security and performance. Furthermore, as the energy consumption is also taken into account in the process of routing, PSGR can satisfy the requirements of both security and energy-efficiency.

Lin et al. [14] proposed a Privacy-Aware Secure Hybrid Wireless Mesh Protocol (PA-SHWMP) to defend against inside attacks in WMNs, and later [15] proposed a role based secure routing protocol. Compared with these previous work [14, 15], this paper offers original and important contributions by 1) taking into account energy consumption in the routing process; 2) considering HWMNs that is more practical and exposed to attacks than WMNs; 3) optimal route selection and route maintenance; 4) malicious node classification and management.

3. BACKGROUND

3.1. Security Model

In this paper, we employ the holistic approach to implement the security and privacy preserving in HWMNs, where two types of security mechanisms work together in a coordinated and adaptive way. One is the preventive security mechanism that attempts to prevent attacks, e.g., cryptography techniques. The other is the reactive security mechanism trying to detect and react against intrusions such as reputation mechanisms.

Every mesh node pre-loads an identity table which provides the information of peering mesh nodes in the network. Each entry of the table describes the identity of a specific mesh node through binding the following information together with the mesh node: MAC address, SL, and valid time period. The trusted identity manager in HWMNs has to reflect the current bindings of mesh nodes in HWMNs and mesh nodes need to contact the identity manager when the service is available to keep the freshness and correctness of the identity table. Every mesh node also pre-loads a local reputation table storing the direct opinion on others and a certain SL based on its hierarchic ranking or the role it plays in HWMNs. A hierarchical key distribution center is pre-loaded in HWMNs where each mesh node pre-loads a key pool and an initial key according to its SL through using the proposed novel hierarchical key management protocol. Each of these keys are hashed using a secure hash function dependent on the key size.

3.2. Adversary Model

HWMNs are vulnerable to both external and internal attacks. External attacks in HWMNs have been well investigated. However, there is not much exploration on the internal attacks in HWMNs, particularly on the security and privacy protection based routing protocol for HWMNs. We focus on two most common internal attacks that are launched by an adversary appearing to be a legitimate participant in the network [16]:

1. Blackhole/Grayhole attack: Blackhole attack and its variant Grayhole attack are the attacks that lead to Denial-of-Service (DoS) in HWMNs. In a Blackhole attack, the malicious node drops all the traffic that is supposed to be forwarded; while in a Grayhole attack, the adversary avoids detection by dropping the packets selectively.

2. Wormhole attack: A wormhole attack aims to prevent discovering route between two legitimate nodes or divert traffic to malicious nodes by establishing a tunnel within two or more malicious collusion nodes. As a result, the malicious nodes are added in the path and then they either drop all the packets resulting in a complete DoS attack, or drop the packets selectively to avoid detection.

The adversary may compromise certain nodes and gain full control of them. Once nodes are captured the attacker can gain access to all stored information, including public keys, private keys. The adversary could also reprogram the captured nodes to behave in a malicious manner. The purposes of the adversary include: 1) DoS attacks (launched via dropping packets) against service availability, 2) illegal and unaccountable network access and 3) the privacy of legitimate network users [12].

3.3. Energy Model

With the aim of improving energy efficiency and prolonging battery life of the mesh client nodes energy consumption is taken into account as an important factor when choosing the best path based on Eq. (5) in the routing protocol design detailed in Section 6.

A multitude of research efforts have been devoted to modelling the energy consumption of wireless networks [17]. Moreover, IEEE 802.11 Distributed Coordination Function (DCF) [18] based Medium Access Control (MAC) protocols have been widely used in wireless ad hoc networks where the energy consumption is a critical issue. In this section, we analyze the energy consumption per successful packet transmission of a client in a WMN using a cost-efficient analytical model [17]. Without loss of generality we consider a scenario of N client nodes. The transmission queue at each client node is modelled as an M/M/1/K queuing system where the traffic follows a Poisson arrival process with rate λ (packets/second), where K represents the buffer size at the client node.

Let e_{tx}, e_{rx}, e_{ov} and e_{id} denote the power required for transmitting, receiving, overhearing and being idle, respectively. The overall energy consumed by a client node to successfully transmit a packet, E, can be decomposed into four components and is given by

$$E = E^{su} + E^{co} + E^{bf} + E^{em} \tag{1}$$

where E^{su} is the energy consumption for a successful packet transmission from the client node, E^{co} is the energy wasted in collisions before the successful transmission, E^{bf} is the energy spent in the backoff stages, and E^{em} is the energy consumed when the client node has no pending packet between any two consecutive transmissions. These components of the energy consumption model can be obtained from [17].

3.4. Subjective Logic

Subjective logic [19] represents a specific belief calculus that uses a belief metric called opinion to express subjective reputation. Since it is necessary to develop mechanisms to detect and manage malicious nodes in WMNs subjective logic with the ability to explicitly represent and manage a nodes uncertainty has emerged as an attractive tool for handling trust relationships in WMNs.

In subjective logic each opinion is denoted by a 4-tuple $\omega_{x:y} = (b_{x:y}, d_{x:y}, u_{x:y}, a_{x:y})$, where $b_{x:y}$, $d_{x:y}$, $u_{x:y}$ designate node *x*'s belief, disbelief and uncertainty towards *y* respectively. The base rate $a_{x:y}$ designates *x*'s willingness to believe *y* which determines how uncertainty is viewed as belief when the reputation is used. The uncertainty reflects the confidence in node *x*'s knowledge of *y*; an uncertainty of 1.0 represents that a node has no basis for any conclusion. They satisfy the following conditions.

$$\begin{cases} b_{x:y} + d_{x:y} + u_{x:y} = 1.0 \\ b_{x:y}, d_{x:y}, u_{x:y}, a_{x:y} \in [0.0, 1.0] \end{cases} \tag{2}$$

When an opinion is used in a decision, it is projected onto the belief/disbelief axis through its expectation, $E(\omega_{x:y})$, which is used to identify malicious nodes and can be computed as

$$E(\omega_{x:y}) = b_{x:y} + a_{x:y} u_{x:y} \tag{3}$$

4. A SUBJECTIVE LOGIC BASED DYNAMIC REPUTATION MECHANISM

In this section, a subject logic based dynamic reputation mechanism (DRM) is presented to defend against the internal attacks, to preserve the privacy of information and to promote a secure and reliable collaboration relationship among participants.

4.1. Dynamic Reputation Mechanism (DRM)

Suppose *x* and *y* are two neighbouring nodes, the final opinion of *x* towards *y* at time t_0, $\omega_{t_0,x:y}^{final}$, includes two components. One is the direct opinion $\omega_{t_0,x:y}^{dir}$;; the other is the recommendation opinions $\omega_{t_0,x:y}^{rec}$.

4.1.1. Direct Opinion

The direct opinion $\omega_{t_0,x:y}^{dir}$, is stored in node *x*'s local reputation table and can be computed as

$$\begin{cases} b_{t_0,x:y}^{dir} = \dfrac{N_{x:y}^{s}}{N_{x:y} \times ((1-\alpha) \times Q_{l(x:y)}^{t_0-1} + \alpha \times \dfrac{T_s^{t_0}}{T_t^{t_0}})} \\ d_{t_0,x:y}^{dir} = \dfrac{N_{x:y}^{f}}{N_{x:y} \times ((1-\alpha) \times Q_{l(x:y)}^{t_0-1} + \alpha \times \dfrac{T_s^{t_0}}{T_t^{t_0}})} \end{cases} \tag{4}$$

where $N_{x:y}$ is the total number of packets that have been transmitted by node *x* to node *y* for forwarding, $N_{x:y}^{s}$ denotes the number of packets that have been successfully forwarded by node *y*, $N_{x:y}^{f}$ is the number of packets that node *y* has not forwarded. $Q_{l(x:y)}^{t_0-1}$ is the evaluation value of the link quality between *x* and *y* during the measurement period of the *(t_0-1)-th* cycle [20]. α is the smoothed constant ($0 < \alpha < 1$). $T_s^{t_0}$ and T_t^{t} are the number of successful transmissions and the total number of transmissions during the measurement period of the *t_0-th* cycle, respectively.

For an entirely unknown node or a new node in DRM there is no basis for any conclusion about belief *b* and disbelief *d* (which means full uncertainty), the default opinion assigned by its neighbours is (0.0,0.0 1.0,0.5), where the willingness to believe *a* is set to be the mean between 0 and 1.

4.1.2. Recommendation and Final Opinion

When there is not enough records of interaction history for node *x* to evaluate the direct opinion towards *y* or the direct opinion is not enough for *x* to make a decision towards *y*, *x* will start a recommendation opinion query by broadcasting a Reputation Query message to the neighbours and waits for a time interval *T*. Whenever one of node *x*'s neighbours receives the Query message it checks its local reputation table to see whether there is a direct opinion towards *y* with the uncertainty value of less than 1.0. If there exists a direct opinion, the neighbour sends a Reply message to *x* containing its *id*, SL and subjective opinion on *y*, otherwise it simply ignores the query.

After receiving the replies *x* will execute the recommendation opinion evaluation phase. Let *R* represent the set of recommenders ($|R| = n, n > 1$), then the recommendation opinion at time t_0 can be calculated by Eqs. (5)-(7) in [15]. After getting the direct opinion and the recommendation opinion, the final opinion at time t_0, $\omega_{t_0,x:y}^{final}$, can be calculated by Eqs. (8)-(10) in [15].

The multi-level security technology [20] is used to classify the malicious nodes and to decide whether and how to punish or isolate the nodes in order to make the malicious nodes management more flexible and to improve the fault-tolerant capability of DRM. Link security aims to authenticate a peer and to establish session keys between two Mesh nodes (MDs) during the transmission process. A hierarchical key management protocol HKMP [15] is used to improve the transmission security for the proposed routing protocol.

5. THE PRIVACY-AWARE, SECURE AND GREEN ROUTING PROTOCOL: PSGR

Fig. 1 illustrates an overview of the SDN-based HWMN. The logically centralized controller implements routing control of the software-defined HWMN with three main modules. The controller interacts with various applications in the upper layer through Northbound APIs, while communicating with data plane (i.e., mesh routers) via Southbound API, e.g., OpenFlow. The main goal of the SDN control plane is to improve the utilization of shared bandwidth, privacy, and energy-efficiency by directing traffic through the HWMN, based on the sharing routing protocol. Therefore, the control plane exposes an interface to the mesh routers for the exchange of routing control

information. We briefly discuss the main control plane modules related to the PSGR routing protocol, which include Reputation Computation, Energy Consumption Modelling, and Hierarchical Key Management, where Reputation Computation module is responsible for computing the reputation of mesh routers; Energy Consumption Modelling module calculates the energy consumption of selected routing path; and Hierarchical Key Management module is to ensure the fine-grained and effective link security.

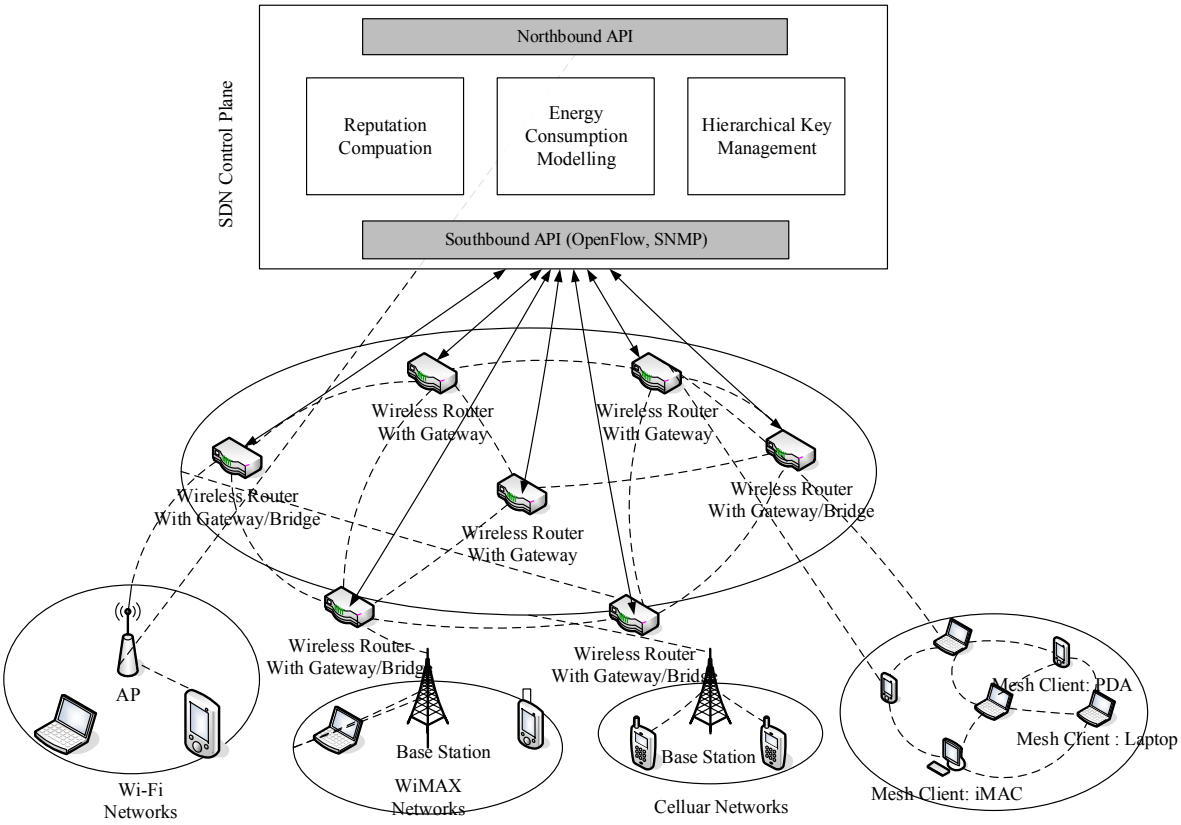

Fig.1. An overview of the SDN-based HWMN

Based on the ideas and methods presented in the previous sections, the privacy-aware, secure and green routing protocol PSGR is detailed in this section as shown in Algorithm 1, which can defend against the internal attacks to achieve stronger privacy protection and also to reduce the energy consumption for HWMNs.

Algorithm 1: Privacy-Aware, Secure and Green Routing Protocol (PSGR)

Input: Source address, destination address, secure and energy requirements,
Output: A meeting all requirements and the most reliable path L_{final} , route maintenance message

1. **Begin**
2. All nodes authenticate their neighbours to generate and distribute keys by using the HKMP protocol;

3. **Route discovery phase:**
4. The source node y broadcasts a *PREQ* message to its neighbours to trigger the route discovery phase described as follows:
5. If node x receives the *PREQ* successfully then
6. x retrieves its direct opinion $\omega_{x:y}^{dir}$ from its local reputation table and calculates the expectation $E(\omega_{x:y}^{dir})$;
7. If ($E(\omega_{x:y}^{dir}) < \gamma_1$) then
8. x considers that y is a malicious node;
9. Else if ($E(\omega_{x:y}^{dir}) > \gamma_2$) then
10. x considers that y is a trustworthy node;
11. Else
12. x broadcasts a reputation *Query* message to the common neighbours asking for their recommendation opinions on node y;
13. Do
14. If ($u_{k:y}^{dir} <1.0$ (k is any node who receives the *Query* message)) then
15. k sends its direct opinion towards y, $\omega_{k:y}^{dir}$, to x;
16. End if
17. While (time interval <T);
18. x weights each received recommendation opinions and integrates them into a recommendation opinion $\omega_{x:y}^{rec}$;
19. x computes the final opinion towards y $\omega_{x:y}^{final}$;
20. If ($E(\omega_{x:y}^{final}) > \gamma_2$) then
21. x considers that y is a trustworthy node;
22. Else
23. x considers that y is a malicious node;
24. End if
25. End if
26. End if
27. If y is considered trustworthy then
28. x sends an *Accept* message including its *ID* to y and records a positive interaction with *y;*
29. Else
30. x sends a *Refuse* message to y and records a negative interaction with *y;*
31. End if
32. x executes the malicious node classification and the management process to make the decision of whether and how to punish or isolate malicious node y.
33. If y receives the *Accept* message successfully then
34. y compares the security levels of x and y;
35. If (g>h) (Suppose that y is deployed at level g and node x is deployed at level h) then
36. y will reject x to be the next forwarding node;
37. Else
38. y will make a decision whether x is the malicious node;
39. If ((x is not the malicious node) && (g=h)) then
40. y computes their pair-wise keys and send a response message back to x;
41. Else if ($1 \le g < h$) then
42. y sends a response message back to x that computes their pair-wise keys;
43. End if
44. End if
45. End if
46. If there are many paths meeting the requirements then
47. The most reliable path denoted as L_{final} is chosen by Eq. (5);
48. End if
49. **End Routing discovery**
50. **Routing reply phase:**
51. The destination node sends a *PREP* message back to the node from which it received the *PREQ* to triggers the route reply phase;
52. The node then forwards the PREP packet along the selected path until it reaches the source node;
53. **End Routing reply**
54. **End**

In PSGR, before starting a route setup process all the mesh nodes authenticate their neighbours to generate and distribute keys. Afterwards, the source node triggers the route discovery phase by constructing a route discovery message *PREQ* labelled with SL indicating the security requirements on the requested route and then broadcast *PREQ* to its neighbours. Let $\gamma_1 and\ \gamma_2$ ($\gamma_1 < \gamma_2,\ \gamma_1, \gamma_2 \in [0.0, 1.0]$) be the minimum and maximum thresholds respectively. The details of the route discovery process are described as follows.

1. The source node *y* broadcasts a *PREQ* message to its neighbours.
2. When one of its neighbours *x* receives the *PREQ* successfully, *x* carries out the DRM to decide whether node *y* is trustworthy by performing the following steps:

   1) Node *x* retrieves its direct opinion $\omega_{x:y}^{dir}$ from its local reputation table and calculates the expectation $E(\omega_{x:y}^{dir})$.

   2) If $E(\omega_{x:y}^{dir}) < \gamma_1$, node *y* is perceived as malicious. If $E(\omega_{x:y}^{dir}) \geq \gamma_2$, *y* is perceived as trustworthy. If $\omega_{x:y}^{dir}$ does not exist or $\gamma_1 < E(\omega_{x:y}^{dir}) < \gamma_2$, node *x* invokes the following reputation query procedure:

      i) Node *x* broadcasts a reputation *Query* to the common neighbour nodes asking for their recommendation opinions on node *y* and waits for a specified time interval *T*.

      ii) Any node *k* whose uncertainty, $u_{k:y}^{dir}$, of its direct opinion towards node *y* is less than 1.0 sends its direct opinion towards *y*, $\omega_{k:y}^{dir}$, to node *x*.

      iii) After the time interval *T* node *x* weights each received recommendation opinions and integrates them into a recommendation opinion $\omega_{x:y}^{rec}$, node x also combines the direct opinion $\omega_{x:y}^{dir}$ with the recommendation opinion $\omega_{x:y}^{rec}$. Finally node *x* obtains the final opinion $\varpi_{x:y}^{final}$.

      iv) After obtaining the final opinion $\varpi_{x:y}^{final}$ node *x* calculates its expectation $E(\varpi_{x:y}^{final})$. If $E(\varpi_{x:y}^{final}) \geq \gamma_2$ node *y* is perceived as trustworthy, otherwise *y* is perceived as malicious.

3. If node *y* is trustworthy then node *x* sends an *Accept* message including its *ID* to *y* and *y(x)* records a positive

interaction with *x(y)*. Otherwise, if node *y* is malicious then *x* sends a *Refuse* message to *y* and records a negative interaction with *y*. Furthermore, *x* executes the malicious node classification and the management process is described in Section 4 to make the decision of whether and how to punish or isolate malicious node *y*.

4. After node *y* receives the *Accept* message successfully, it compares the security levels of two nodes. Suppose that *y* is deployed at level *g* and node *x* is deployed at level *h*. If $g>h$, *y* will reject *x* to be the next forwarding node; otherwise *y* will execute Steps 2 and 3 to make a decision whether *x* is the malicious node. If *x* is not the malicious node and $g=h$, *y* will compute their pair-wise keys and send a response message back to *x*, if $1 \le g < h$ then *y* sends a response message back to *x* that will compute their pair-wise keys.

5. Repeated Steps 2, 3, and 4 until the satisfying terms of path are found.

6. If there are many paths meeting the requirements, the most reliable path denoted as L_{final} is chosen based on the rules below.

$$\begin{aligned} & L_{final} = Max\left(\varphi_{i1} * \varpi_{L(i)} + \varphi_{i2} * SL_{L(i)}\right), i = 1 \quad n \\ & s.t. \\ & \qquad \varphi_{i1} + \varphi_{i2} = 1 \\ & \qquad Th_1 < E_{L(i)} < Th_2 \end{aligned} \tag{4}$$

where $L_{(s)}, (s = 1 \quad n)$, is the set of the paths meeting the minimum security needs. φ_{i1} and φ_{i2} are the weight factors corresponding to the opinion and security level of path $L_{(i)}$, respectively. Th_1 and Th_2 are the thresholds of $E_{L(i)}$. $\varpi_{L(i)}$ and $SL_{L(i)}$ are the opinion and security level of path $L_{(i)}$, respectively. $E_{L(i)}$ is the energy consumption of path $L_{(i)}$. $\varpi_{L(i)}$, $SL_{L(i)}$ and $E_{L(i)}$ can be given by

$$\begin{cases} \varpi_{L(i)} = Min\left(\sum_{j=1}^{m} \varpi_j^i \Big/ m,\ \min(\varpi_j^i)\right) \\ SL_{L(i)} = Min\left(SL_j^i\right) \\ E_{L(i)} = m * Max(\sum_{j=1}^{m} E_j^i \Big/ m, \max(E_j^i)) \end{cases} \tag{5}$$

where N_j^i ($N_j^i \in L_{(i)}, j = 1 \quad m$) is the *j*-th node in the *i*-th path $L_{(i)}$. ϖ_j^i and SL_j^i are the opinion and security

level of node N_j^i, respectively. E_j^i is the energy consumption of node N_j^i.

When the destination node receives the route discovery message it triggers the route reply phase by sending a *PREP* message back to the node from which it received the *PREQ*. The node then forwards the *PREP* packet along the selected path until it reaches the source node.

6. SECURITY ANALYSIS AND EXPERIMENTAL EVALUATION

6.1. Security Analysis

In this paper the security and privacy protection are implemented through the dynamic reputation mechanism, a reputation based node security rating scheme and a multi-level hierarchical key management protocol.

Firstly, the dynamic reputation mechanism is able to achieve efficient identification and management of malicious nodes and to defend against internal attacks in the process of route selection by dynamically evaluating the node's reputation. The reputation is derived from the historical interactions as well as the neighbours' recommendations.

Secondly, the privacy information and the nodes are divided into different levels according to the security requirements and the node's reputation. Then, with the reputation based node security rating scheme and the multi-level hierarchical key management protocol, each node is assigned with a security level and a session key accordingly. The node with the assigned security level and session key is only allowed to participate in the network and access the privacy information according to its security level, which can further improve the capability of internal attacks defence, especially those launched by the unidentified malicious nodes. Moreover, the data will be delivered to the correct receiver without revealing any privacy information.

Thirdly, the multi-level hierarchical key management scheme is used to protect the non-mutable fields and mutable fields in the routing messages respectively, which further improve the privacy by strictly restricting user

access to the resources. In what follows, we discuss the security features of PSGR considering Blackhole/Grayhole attacks and wormhole attacks.

In the route selection process, the dynamic reputation mechanism coupled with the node security rating scheme and the node's security level can effectively identify and manage the malicious node, making sure that only those nodes meeting the security requirement embedded in the packets can participate in the route discovery phase. Also, by encrypting and authenticating certain fields, the malicious nodes with the lower security level can be prevented from modifying and interpreting the packets without the higher-level key.

During the packet transmission process we consider that in the given routing path there are some unidentified malicious nodes included or some normal nodes compromised. According to the features of the Blackhole/Grayhole and wormhole attacks they will launch the attacks by dropping packets. Once they start dropping packets they will be detected by the route maintenance phase through dynamically monitoring the relaying node forwarding behaviour and the upstream/downstream traffic. Therefore the malicious nodes will be forced to cooperate or be isolated by the proposed malicious node classification and management scheme.

Equipped with the aforementioned protection features the Blackhole/Grayhole and wormhole attacks can be effectively prevented in both the route selection and the packet transmission process. The packets as well as the privacy information are protected from insiders and can only be recognized by legitimate mesh nodes and opened by the expected destination mesh node. Furthermore, PSGR can also improve route robustness and fault tolerance by providing more route choices through multi-level route discovery and maintenance. For instance if a route at a certain security level is broken the source node can still communicate with the destination node using another route at other security levels.

6.2. Experimental Evaluation

OPNET [21] simulation experiments were conducted to demonstrate the performance and energy efficiency of the PSGR protocol. The simulation area is 1000 m * 1000 m with 50 nodes in total. There are 4 nodes contending

for transmission within each hop. The physical layer uses a fixed transmission range model where two nodes can directly communicate with each other only if they are within a certain transmission range, i.e., within a hop. The MAC layer protocol uses the IEEE 802.11 Distributed Coordination Function (DCF) [18]. The arrival traffic at each MN has a Constant Bit Rate (CBR) with rate 1 Mbps and a packet size 1024 bytes. The channel data rate is 10 Mbps and each MN has a buffer size of 25 packets. The other MAC and Physical layer parameters follow the existing study [15]. The security parameters $\alpha, \beta, \gamma_1, \gamma_2, \eta_1, \eta_2$ are 0.5,0.5,0.3,0.6,0.3,0.7, which are empirical values obtained from multiple experiments. The experimental network topology graph is shown in Fig. 2. Each data point depicted in Figs. 3-7 is the average of the results obtained from 20 runs of simulation experiments with a simulation time of 100 s.

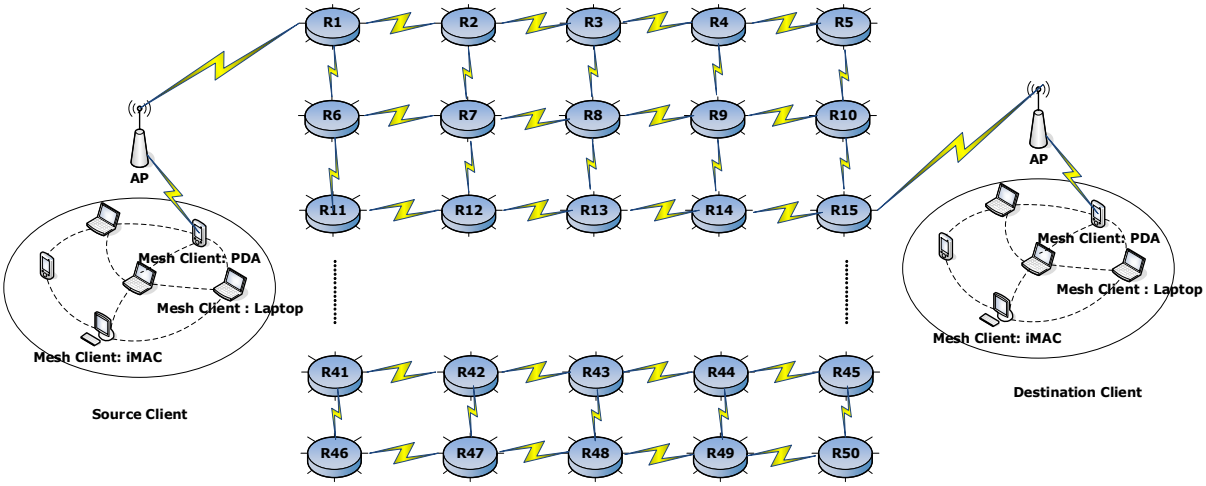

Fig. 2. The experimental network topology graph

6.2.1. Performance of the PSGR Routing Protocol

The performance of the PSGR is compared to the PA-SHWMP [14], PASER [22] and HWMP in terms of the following performance metrics when Blackhole/Grayhole attacks and wormhole attacks are present [23].

- *Average throughput*: the ratio of the number of packets that successfully reach destinations to the number of packets generated at sources.
- *Packet delivery ratio (PDR)*: the ratio of the number of packets that are successfully received and accepted at destinations to the number of packets generated at sources.

- *End-to-end delay (ED)*: the average time duration experienced by a packet transmitted from a source to a destination.

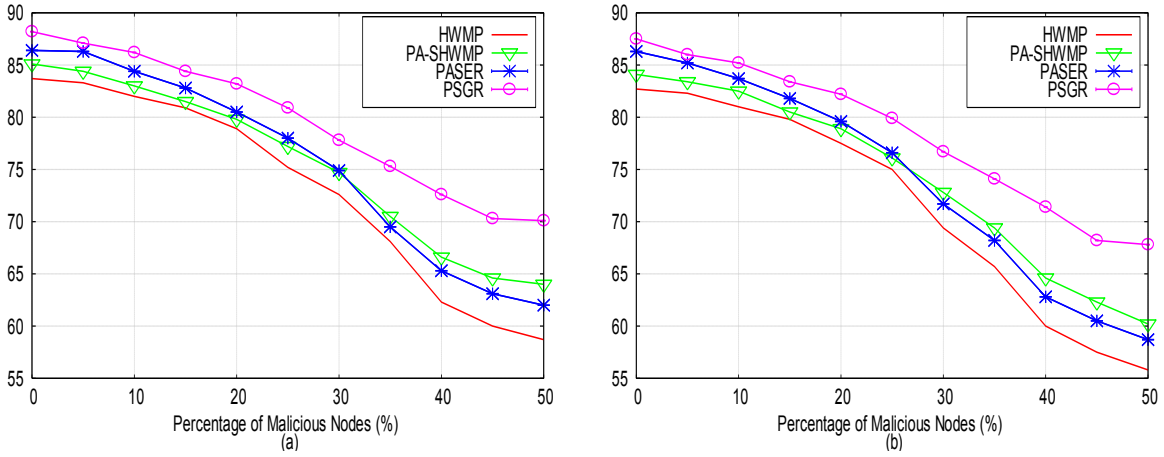

Fig. 3. Average Throughput: (a) Blackhole/Grayhole Attacks (b) Wormhole Attacks

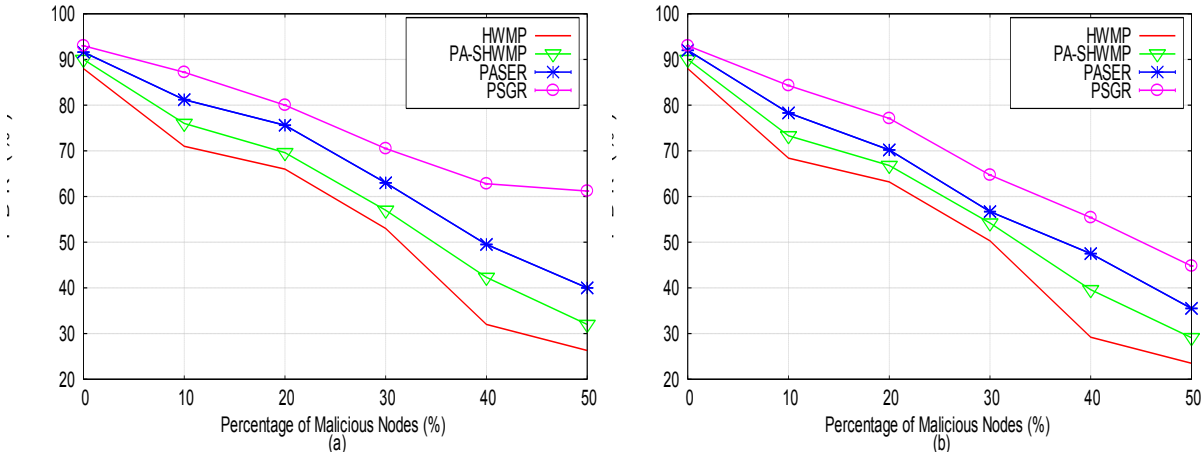

Fig. 4. Average PDR: (a) Blackhole/Grayhole Attacks (b) Wormhole Attacks

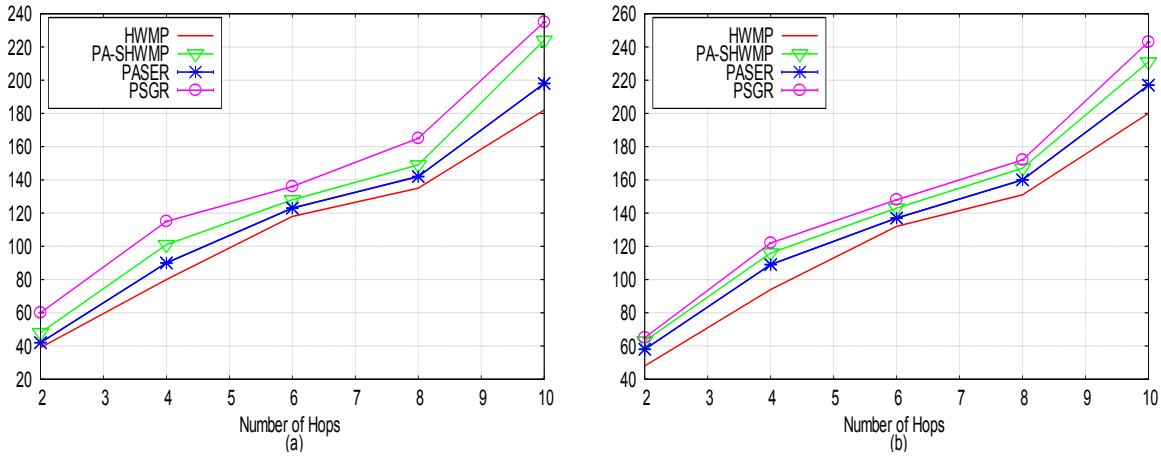

Fig. 5. Average ED: (a) Blackhole/Grayhole Attacks (b) Wormhole Attacks

(1) Average Throughput

As shown in Fig. 3 the average throughputs of all the three protocols are affected by the presence of malicious nodes in both Blackhole/Grayhole and wormhole attacks. Since HWMP does not take into account the internal attacks and internal malicious nodes its performance is degraded most. For PA-SHWMP, PSGR and PASER, since they establish the route based on the reputation mechanism and hybrid cryptosystem, which can identify and avoid the malicious nodes participating in the routing, their performance reductions are less than that of the HWMP. In PASER, the routing communication security relies on the origin, neighbor authentication and dynamic key management scheme. When the percentage of malicious nodes is less than 30 percent, most of the authenticated nodes are normal and they actively engage in the routing and data forwarding, which makes the throughput of the PASER better than that of the PA-SHWMP. For PSGR, the proposed dynamic reputation mechanism updates the node status effectively and rapidly, which enables PSGR to identify and isolate more malicious nodes than the PASER and thus achieves a better throughput. When the percentage of malicious nodes is greater than 30 percent, more internal nodes have been captured. Because of the lack of the rapid identification of internal malicious nodes, the management and node status update schemes, the PASER cannot exclude the malicious nodes from the routing and data forwarding, so the throughput of the PASER is less than that of the PA-SHWMP and PSGR. Moreover, since the dynamic reputation mechanism proposed in PSGR is more flexible and accurate than the static reputation mechanism used in PA-SHWMP, the performance of PSGR in better than that of PA-SHWMP.

(2) Average Packet Delivery Ratio (PDR)

The results in Fig. 4 reveal that the PDR of the network decreases as the number of malicious nodes increases. However, the PDR under PSGR is better than those under PA-SHWMP, PASER and HWMP. HWMP does not take into account internal attacks and malicious nodes and therefore cannot avoid malicious nodes participating in the routing, thus its PDR is the worst. In PA-SHWMP and PASER, the malicious nodes are excluded from the network soon after they have been detected, which results in less nodes that can participate in the routing and thus the PDR of PA-SHWMP and PASER decreases rapidly as the number of malicious nodes increases. However, in PSGR, the

dynamic reputation mechanism identifies the malicious nodes more accurately than the PA-SHWMP and PASER. Furthermore, when the malicious nodes have been detected the flexible malicious node classification and management scheme is adopted to make the decision on whether and how to punish or isolate the node. This ensures that only those malicious nodes with low security levels will be excluded from the network and others will be forced to cooperate. Therefore, the more accurate identification of malicious nodes and the larger number of cooperating nodes lead to the better PDR performance of PSGR than that of PA-SHWMP and PASER.

(3) Average End-to-End Delay (ED)

The simulation experiment was conducted using 5 to 10 source-destination pairs to compare the average ED of the four protocols. As shown in Fig. 5, with light or medium traffic loads and less hops the delay is less than 200ms, whereas under heavy traffic loads and more hops the delay reaches nearly 250ms. The average ED is slightly higher in PSGR than those in PA-SHWMP, PASER and HWMP, because in addition to the routing operation of HWMP, the PSGR, PASER and PA-SHWMP also require to execute the routing security mechanism to detect and isolate the malicious nodes, which results in a higher delay. Moreover, the PSGR performs another two effective schemes to provide privacy preservation and to reduce energy consumption, respectively. As a result, the average ED in PSGR is slightly higher than those of PA-SHWMP, PASER and HWMP as a trade-off for the better throughput, PDR and energy efficiency.

6.2.2. Energy Consumption

In this subsection, we evaluate and compare the energy consumption of the PSGR to those of PA-SHWMP, PASER and HWMP.

(1) Average Energy Consumption

The results shown in Fig. 6 are obtained from simulation experiments with 2 to 15 source-destination pairs to compare the average energy consumption of PSGR, PA-SHWMP, PASER and HWMP. Fig. 6 shows that the average energy consumption is dramatically affected by the number of hops. As the number of hop increases the

average energy consumption of all the four protocols increases. However, since the energy consumption is taken into account in the process of routing, the PSGR is more energy-efficient than the PA-SHWMP, PASER and HWMP.

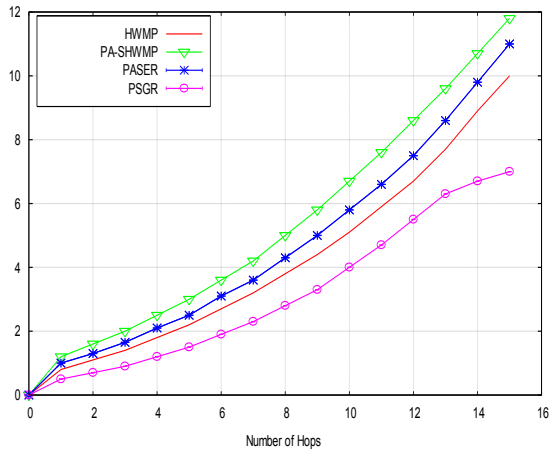

Fig. 6. Average Energy Consumption

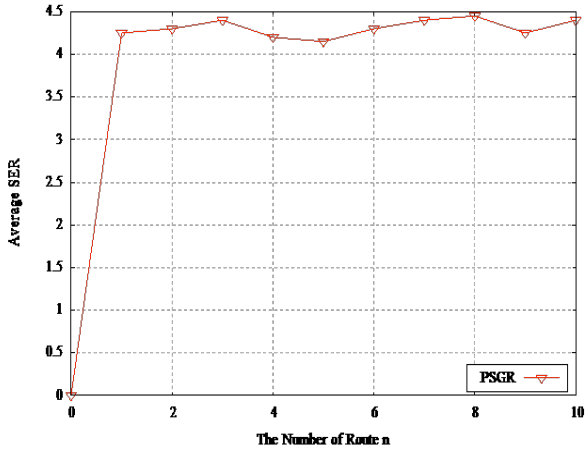

Fig. 7. Average SER

(2) Average SER

Let *R*, *SL* and *E* denote the set of the routes, the security level and the energy consumption level of the routes in *R*, respectively. Then we classify *SL* and *E* into 5 levels to separately denote the corresponding security levels (*SL*) and the energy consumption levels (*E*). Therefore, each route in set *R* can be denoted by a 2-tuple $R(i) = (SL_{R(i)}, E_{R(i)}), (SL_{R(i)}, E_{R(i)} = 1 \quad 5)$, where $SL_{R(i)}$ and $E_{R(i)}$ denote the security level and the energy consumption level of the route $R(i)$, respectively. Based on the above definition, a new metric, SER, is proposed to evaluate the energy consumption of the PSGR,

$$SER_{R(i)} = \frac{SL_{R(i)}}{E_{R(i)}} \tag{6}$$

In Fig. 7, we depict the average SER against the number of routes, *n*, which satisfies the requirements of both security and energy consumption. As shown in Fig. 7, the SER of the selected route in all cases is near 85% of the highest SER. The results indicate that the proposed route discovery scheme can satisfy the requirements of both security and energy consumption.

7. CONCLUSIONS

In this paper, we have investigated the pressing problems such as privacy preserving, route security and energy consumption in Software defined HWMNs and have proposed a privacy-aware, secure and green routing protocol, PSGR. Based on the combination of the proposed dynamic reputation mechanism and a multi-level hierarchical key management protocol, the PSGR protocol can effectively defend against the internal attacks to provide privacy protection in HWMNs. Moreover, by taking the energy consumption into the process of routing, the PSGR protocol can achieve good energy efficiency. The elaborated theoretical analyses have verified that the PSGR is secure, privacy preserving and efficient. Furthermore, simulation experiments have demonstrated that in the presence of the Blackhole/Grayhole attacks and wormhole attacks, the packet delivery ratio, network throughput and energy consumption of the proposed PSGR are much better than those of the PA-SHWMP, PASER and HWMP routing protocols.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (61472083, 61402110, 61402262, U1405255), the Fujian Normal University Innovative Research Team (IRTL1207), the UK EPSRC research grant (EP/M013936/2), the Foundation of Science and Technology on Information Assurance Laboratory (KJ-14-109), the Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund, and the Pilot Project of Fujian Province (formal industry key project) (2016Y0031).

REFERENCES

1. I. Ouveysi, K. C. Wong, S. Chan, K. T. Ko, “Interface assignment-based aodv routing protocol to improve reliability in multi-interface multichannel wireless mesh networks”, *Mobile Information Systems*, vol. 9,pp.1-16,2015.
2. I.F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: A Survey”, *Computer Networks*, vol. 47,

no. 4, pp. 445-487, 2005.

3. J. Sen, “Security and Privacy Issues in Wireless Mesh Networks: A Survey”, *Wireless Networks and Security*, Springer Berlin Heidelberg, pp. 189-272, 2013.

4. S. Paris, C. N. Rotaru, F. Martignon, A. Capone, “Cross-Layer Metrics for Reliable Routing in Wireless Mesh Networks”, *IEEE-ACM Transactions on Networking*, vol. 21, no. 3, pp. 1003-1016, 2013.

5. G．Sato, N. Uchida, Y. Shibata, “Resilient Disaster Network Based on Software Defined Cognitive Wireless Network Technology”, *Mobile Information Systems*, vol. 10,pp.1-11,2015.

6. H. Huang, P. Li, S. Guo, W. Zhuang, “Software-defined wireless mesh networks: architecture and traffic orchestration”, IEEE Network, vol.29, no.4, pp.24-30, 2015.

7. S. Khan, N.A. Alrajeh, and K.K. Loo, “Secure Route Selection in Wireless Mesh Networks”, *Computer Networks*, vol. 56, no. 2, pp. 491-503, 2012.

8. R. Riggio, T. Rasheed, S. Sicari, “Performance Evaluation of an Hybrid Mesh and Sensor Network”, *Proc. IEEE Globecom*, 2011.

9. F. Nait-Abdesselam, B. Bensaou, and T. Taleb, “Detecting and Avoiding Wormhole Attacks in Wireless ad hoc Networks”, *IEEE Communication Magazine*, vol. 46, no. 4, pp. 127–133, 2008.

10. S. Paris, C.N. Rotaru, F. Martignon and A. Capone, “EFW: A Cross-Layer Metric for Reliable Routing in Wireless Mesh Networks with Selfish Participants”, *Proc. IEEE INFOCOM*, Shanghai, China, 2011.

11. M.S. Islam, M.A. Hamid and C.S. Hong, “SHWMP: A Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s Wireless Mesh Networks”, *IEEE Transactions on Computational Science VI*, vol. 5730, pp. 95-114, 2009.

12. K. Ren, S. Yu, W. Lou, and Y. Zhang, “PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks”, *IEEE Transactions On Parallel And Distributed Systems*, vol. 21, no. 2, pp. 203-215, 2010.

13. S. Khan and J. Loo, “Cross Layer Secure and Resource-Aware On-Demand Routing Protocol for Hybrid Wireless Mesh Networks”, *Wireless Personal Communications*, vol. 62, no. 1, pp. 201–214, 2012.

14. H. Lin, J. Ma, J. Hu and K. Yang, “PA-SHWMP: A Privacy-aware Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s Wireless Mesh Networks”, *EURASIP Journal on Wireless Communications and Networking*, vol. 69, no. 1, pp. 1-16, 2012.

15. H. Lin, J. Hu, J. Ma, L. Xu, and A. Nagar, “A Role Based Privacy-Aware Secure Routing Protocol for Wireless Mesh Networks”, *Springer Wireless Personal Communications*, vol. 75, no. 3, pp. 1611-1633, 2014.

16. S. Dietzel, J. Petit, G. Heijenk, F. Kargl, “Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols”, *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1505-1518, 2013.

17. Jia Hu, Geyong Min, and Mike E. Woodward, “Performance Analysis of the TXOP Burst Transmission Scheme in Single-Hop Ad Hoc Networks with Unbalanced Stations”, *Computer Communications*, vol. 34, no. 13, pp. 1593–1603,2011.

18. IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 1999.

19. Yining Liu, Keqiu Li, Yingwei Jin, Yong Zhang, Wenyu Qu, “A Novel Reputation Computation Model based on Subjective Logic for Mobile Ad Hoc Networks”, *Future Generation Computer Systems*, vol. 27, no. 5, pp. 547-554, 2011.

20. W. P. Lu and MK Sundareshan, “A Model for Multilevel Security in Computer Networks”, *IEEE Transaction on Software Engineering*, vol. 16, no. 6, pp. 647–659,1990.

21. A. S. Sethi and V. Y. Hnatyshin. “The Practical OPNET User Guide for Computer Network Simulation”, CRC Press, 2012.

22. M.Sbeiti, N.Goddemeier, D.Behnke, and C.Wietfeld, " Paser: secure and efficient routing approach for airborne mesh networks", *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1950-1964. 2016.

23. M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 736-745. 2009.

Biography of Authors

Hui Lin received his Ph.D. degree from Xidian University, in 2013. He is currently an Associate Professor and master supervisor at Fujian Normal University. His research interests include wireless and mobile computing systems and network and information security, etc.

Jia Hu is a Lecturer in Computer Science at the University of Exeter. He has published over 40 research papers in prestigious international journals and at reputable international conferences. His research interests include performance evaluation, next generation networking, resource allocation and optimization, energy-efficiency, network security, smart city, and big data.

Li Xu received his Ph.D. degree from Nanjing University of Posts and Telecommunications in 2004. He is currently a Professor and Doctoral Supervisor at Fujian Normal University. His research interests include wireless and mobile computing systems, network and information security, complex networks and systems, intelligent information in communication networks, etc.

Youliang Tian received the PhD degree in cryptography from Xidian University in 2012. He is a professor and master supervisor in College of Computer Science & Technology at Guizhou University. His current research interests include algorithm game theory, cryptography and secure protocol.

Lei Liu an associate professor in Shandong University, China. He has published over 30 papers in conference proceedings and journals. He has served as program committee for more than 20 international conferences, and served as leading guest editor for 5 journal special issues. His current research interests include: software defined networking, 5G, traffic engineering and network big data.

Stewart Blakeway is a Lecturer in Computer Science. He received his PhD in Mobile Ad-Hoc Networks with Cognitive Attributes from Liverpool John Moores University in 2015, his Masters degree with Distinction from University of Liverpool in 2007 and BPhil degree from University of Liverpool in 2001. His main area of research is in Cognitive Wireless Mobile Data Communication Networking.