EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks

Hui Lin[1,2*], Jianfeng Ma[1], Jia Hu[3] and Kai Yang[1]

Abstract

Wireless mesh networks (WMNs) have emerged as a key technology for next generation wireless networks and provide a low-cost and convenient solution to the last-mile problem. Security and privacy issues are of paramount importance to WMNs for their wide deployment and for supporting service-oriented applications. Moreover, to support real-time services, WMNs must also be equipped with secure, reliable, and efficient routing protocols. Therefore, a number of research studies have been devoted to privacy-preserving routing protocols in WMNs. However, these studies cannot defend against inside attacks effectively, often take it for granted that every internal node is cooperative and trustworthy, and rarely consider dividing the user privacy information into different categories according to the security requirements. To address these issues, we propose a Privacy-Aware Secure Hybrid Wireless Mesh Protocol (PA-SHWMP), which combines a new dynamic reputation mechanism based on subject logic and uncertainty with the multi-level security technology. PA-SHWMP can defend against the internal attacks caused by compromised nodes and achieve stronger security and privacy protection while maintaining reasonable balances between security and performance. We analyze the PA-SHWMP protocol in terms of security, privacy, and performance. The simulation results show that the packet delivery ratio of the proposed PA-SHWMP becomes better than that of the existing HWMP and SHWMP protocols, when the number of malicious nodes and the percentage of lossy links increase. Moreover, the convergence time of PA-SHWMP is smaller than HWMP and SHWMP with any percentage of malicious mesh routers.

Keywords: privacy protection, wireless mesh networks, routing

1. Introduction

Wireless mesh networks (WMNs) have emerged as a key technology for the next generation wireless network and provide a low-cost and convenient solution to high-speed Internet access and applications such as web surfing, e-banking, e-commerce, teleconferencing, etc. [1,2].

WMNs consist of mesh routers (i.e., nodes) and mesh clients (i.e., users), where the mesh routers form the wireless backbone network and interwork with the wired network to provide multi-hop wireless high-bandwidth connectivity to mesh clients. Mesh clients connect directly to the routers or form wireless adhoc networks to extend the wireless connectivity [3]. Figure 1 shows the network architecture of a 802.11s WMN [4]. A mesh point (MP) is an IEEE 802.11s entity that mainly acts as a relay mesh router. A mesh access point (MAP) is an MP that can also work as an access point. A wireless mobile station (STA) acts as a mesh client and is connected to an MAP through generic WLAN protocols. Mesh portal is also an MP that has a bridging functionality connecting the mesh network to other networks such as a traditional 802.11 WLAN or a non-802.11 network and acts as the gateway router to the WMN infrastructure. WMNs have the advantages of low costs, self-organization, auto-configuration, good scalability, high robustness, etc.

Security and privacy issues are of paramount importance to WMNs for their wide deployment. In WMNs, there are two types of privacy concerns: data- and context-oriented concerns. Data-oriented concerns focus on

* Correspondence: hawkhui95@gmail.com
[1]School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, 710071 China
Full list of author information is available at the end of the article

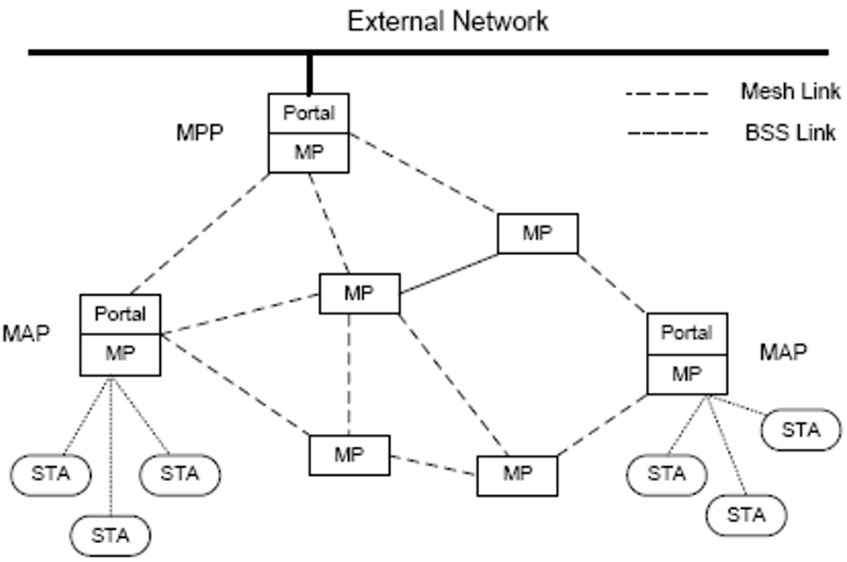

Figure 1 Architecture of a 802.11s WMN.

protecting the privacy of data content collected from, or query posted to, a WMN. On the other hand, context-oriented concerns concentrate on protecting contextual information, such as the location and timing of traffic flows in a WMN [5]. Both privacy concerns may be violated by data and traffic analysis attacks. As illustrated in Figure 2, in data analysis attacks, a malicious mesh router decrypts data to compromise the payload being transmitted. In traffic analysis attacks, a third-party adversary eavesdrops the wirelessly transmitted data and tracks the traffic flow hop-by-hop [5].

Data- and context-oriented privacy concerns may both be threatened by external and internal adversaries. External adversary eavesdrops the data communication between mesh routers in a WMN. Internal adversary is a participating mesh router captured and manipulated by malicious entities to compromise private information. External adversary can be effectively defended against by the traditional cryptographic encryption and authentication techniques. As to internal adversary, since a participating mesh router is allowed to decrypt data legally, the traditional encryption and authentication techniques may no longer be effective.

To address the aforementioned privacy protection challenge and to support real-time applications and smooth delivery of broadband services, WMNs must also be equipped with secure, reliable, and efficient routing protocols. However, security in routing or forwarding functionality is not specified in 802.11s-based WMN. The study in [4] identifies that existing Hybrid Wireless Mesh

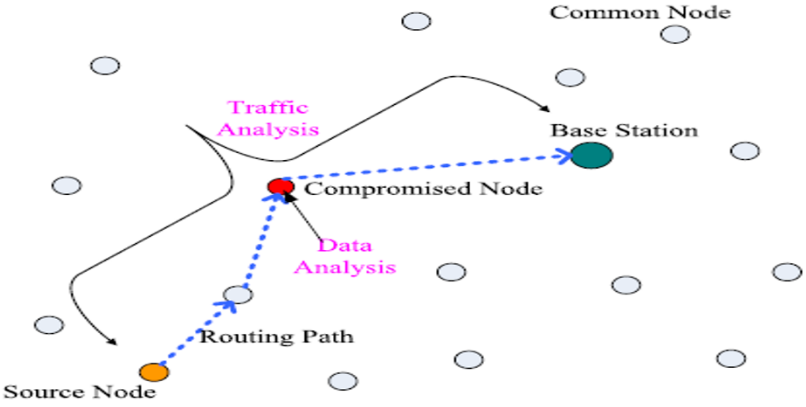

Figure 2 Privacy attacks in WMNs.

Protocol (HWMP) is vulnerable to various types of routing attacks. The main reason is that the intermediate mesh routers need to modify routing messages before forwarding and re-broadcasting them. Furthermore, due to the intrinsically open and distributed nature, WMNs are subject to various attacks from inside [3,6].

In this article, we propose a Privacy-Aware Secure Hybrid Wireless Mesh Protocol (PA-SHWMP), which combines a new dynamic reputation mechanism based on subject logic [7,8] and uncertainty [9] with multilevel security (MLS) technology [10,11].

PA-SHWMP is an improvement of SHWMP introduced by Islam et al. [4]. SHWMP uses cryptographic extensions to provide authenticity and integrity to HWMP routing messages and prevents unauthorized manipulation of mutable fields in the routing information elements. However, SHWMP is vulnerable to the attacks launched by the internal legitimate mesh routers. First, it assumes that all internal mesh routers cooperate with each other without interrupting the operation of protocol. Second, SHWMP uses a hop-by-hop authentication mechanism to provide security of the routing messages. Each mesh router decrypts received packets and re-encrypts them using its own key. In this scheme, the user privacy information is partly protected from eavesdroppers but known by mesh routers because of routing in the mesh backbone. Thus, an active attacker can compromise and control mesh routers to get the user privacy information. Different from SHWMP, PA-SHWMP relies on a hybrid usage of reputation mechanism built by subject logic and user privacy information classification mechanism according to MLS. By providing scalable security services to assure the authenticity, integrity, and secrecy of routing messages, PA-SHWMP can defend against the internal attacks caused by compromised mesh routers and achieve stronger security and privacy protection while maintaining reasonable balance between security and performance.

The rest of the article is organized as follows. We discuss a related study in Section 2. Introductions to subject logic and MLS are described in Section 3. Subsequently, the implementation of PA-SHWMP is given in Section 4. After that, the security and performance analysis are given in Section 5 and 6, respectively. Finally, we draw the concluding remarks in Section 7.

2. Related study

WMNs have become an important focus area of research owing to their promise in providing high-speed wireless connectivity everywhere and realizing numerous next-generation wireless services. Recently, research in WMNs has focused on developing high performance communication protocols. However, given the wireless and multi-hop nature of communication, WMNs are subject to a wide range of security and privacy threats.

Therefore, designing a secure, efficient, and privacy-protection routing protocol for WMNs is a big challenging task. So far, there has been tremendous research on secure routing for wireless networks such as adhoc networks or wireless sensor networks. However, they cannot provide specific security features for mesh networks and are still vulnerable to various types of routing attacks such as gray hole, route re-direction, spoofing, etc [12].

Capkun et al. [13] proposed a privacy-preserving scheme for hybrid adhoc networks, which are exactly WMNs. In the proposed scheme, each mobile node uses temporary public key pairs to establish pairwise secrets with its neighbors and the pairwise secrets in turn are used to build secure route. The scheme is unlikely to provide privacy protection for two reasons. First, some user privacy information has to be disclosed to access points, which makes malicious access point be able to track a specific mobile user. Second, within a time slot the pseudonyms of source and destination keep unchanged, so an adversary can link messages by them. Wu and Li [14] introduced a new structure named as “Onion ring” for WMNs. The scheme uses “Onion encryption” in a ring structure to avoid an adversary to distinguish the source and the destination nodes and to identify the misbehaving mesh routers. However, how to anonymously build the ring in the first place is not mentioned and topology dynamics may make it inefficient. In [15], a penalty-based shortest path routing protocol is proposed to achieve well-maintained balance between network performance and traffic privacy preservation. The scheme is only designed to use multiple paths for data delivery so that an adversary who is only able to observe a fraction of the traffic cannot obtain any meaningful information [3]. Samad and Makram [16] proposed a protected neighborhood-based trust mechanism in clustered WMNs. The mechanism is based on neighborhood trust to gain required security and identification privacy in a clustered WMN. However, some privacy information of users has to be disclosed to the relay mesh routers, which makes malicious mesh routers be able to get the privacy information. Ren et al. [17] proposed PEACE, a novel privacy-enhanced yet accountable security framework, tailored for WMNs. PEACE is presented as a suite of authentication and key agreement protocols built upon short group signature variation. However, PEACE only secures the network from external attacks and takes it for granted that every internal node is cooperative and trustworthy. Sen [18] presented an efficient and reliable routing protocol that also provides user anonymity in WMNs. By robust estimation wireless link quality and the available bandwidth in the wireless route and exploiting the benefits of using multi-point relays and circular routing technique, the protocol is able to sustain a high level of throughput with a low control overhead. The user privacy is protected by using a novel anonymized authentication protocol. However, the proposed routing protocol cannot defend against inside attacks, in which two malicious nodes advertise in such a way as if they have a very reliable link between them.

From the analysis above, it can be summarized that the aforementioned work cannot effectively solve the privacy-related security problem of WMNs. What's more, the intrinsically open and distributed nature of WMNs raise some new privacy security challenges caused by inside attacks, which are neglected by the previous studies.

3. Preliminaries

This section briefly describes subject logic and MLS used in PA-SHWMP.

3.1. Subject logic

Most of the routing protocols in WMNs assume that mesh routers are cooperative and trustworthy. In fact, some routers in WMNs behave maliciously by eavesdropping and decrypting the wirelessly transmitted data, which will cause a great threat on user's privacy and can lead to devastating consequences. Also, they behave selfishly by dropping packets originating from other mesh routers and only forwarding its own packets, to increase their share of available bandwidth. Consequently, it is necessary to develop some mechanisms to detect and isolate selfish and malicious nodes.

Reputation scheme is one of the techniques adopted to detect and isolate selfish and malicious nodes in WMNs. In reputation-based schemes, a node's behavior is measured by its neighbors using a watchdog mechanism [9]. However, cooperative nodes sometimes are perceived as being selfish or malicious due to unreliable transmission in wireless networks. To deal with this issue, Jøsang et al. [19] proposed a method based on subjective logic for discovering trust networks between specific parties and Kane and Browne [7] successfully transplanted and applied subjective logic to a wireless network environment.

Derived from the Dempster-Shafer theory [20] and with the ability to explicitly represent and manage a node's uncertainty, subjective logic emerges as an attractive tool for handling trust relationships in WMNs. Subjective logic represents a specific belief calculus that uses a belief metric called opinion to express subjective beliefs. In subjective logic [7,8], each opinion is denoted by a 4-tuple $\omega_{x:y} = (b_{x:y}, d_{x:y}, u_{x:y}, a_{x:y})$, where $b_{x:y}$ represents node x's belief in node y, $d_{x:y}$ represents node x's disbelief in node y, $u_{x:y}$ represents node x's uncertainty in node y, and the base rate $a_{x:y}$ represents node x's willingness to believe node y, which determines how uncertainty is viewed as belief when the opinion is used. They satisfy the following conditions:

$$\begin{cases} b_{x:y} + d_{x:y} + u_{x:y} = 1.0 \\ b_{x:y}, d_{x:y}, u_{x:y}, a_{x:y} \in [0.0, 1.0] \end{cases} \tag{1}$$

The opinion space can be mapped into the interior of an isosceles triangle, where, for an opinion $\omega_x = (b_x, d_x, u_x, a_x)$, the three parameters b_x, d_x, and u_x determine the position of the vertices accordingly. Figure 3 illustrates an example where the opinion about a proposition x from a binary state space with the value $\omega_x = (0.7, 0.1, 0.2, 0.5)$ [7].

Belief and disbelief can be calculated by the collected evidence. The uncertainty reflects the confidence in node x's knowledge on node y; an uncertainty of 1.0 represents that a node has no basis for any conclusions. The base rate represents node x's willingness to believe node y, which determines how uncertainty is viewed as belief when the opinion is used. When an opinion is used in a decision, it is projected onto the belief/disbelief axis through its expectation $E(\omega_{x:y}) = b_{x:y}+a_{x:y}u_{x:y}$. A base rate of 0.0 causes uncertainty viewed as disbelief, while a base rate of 1.0 causes uncertainty viewed as belief. A base rate of 0.5 causes uncertainty viewed positively as actual belief.

In this article, we will use a base rate of 0.5, so that unknown nodes are by default assigned a median level of trust. For example, if an opinion is (0.6, 0.2, 0.2, 0.5), its expectation can be calculated as $E(\omega_{x:y}) = b_{x:y}+a_{x:y}u_{x:y} = 0.6+0.5*0.2 = 0.7$. An entirely uncertain opinion, $(0.0, 0.0, 1.0, a_x)$ will always have an expectation equal to the base rate, as $E(\omega_{x:y}) = b_{x:y}+a_{x:y}u_{x:y} = 0.0+1.0*a_{x:y} = a_{x:y}$. The base rate then becomes the default opinion for unknown nodes.

3.2. MLS

In Defense Information System Agency (DISA), MLS is defined as a security system containing information with different security levels (SLs) and permits for simultaneous access by users. MLS systems are considered as one of the most secured systems, since it has overcome the operational limitations imposed by system-level operations. MLS includes five rules as follows [10].

- An information system can store information about different classifications.
- Users may have different authorizations and need to know the permits to process information.
- Users cannot access information for which they do not have authorization, or do not need to know.
- A subject can read from an object only if the subject's SL is not lower than the object's SL.

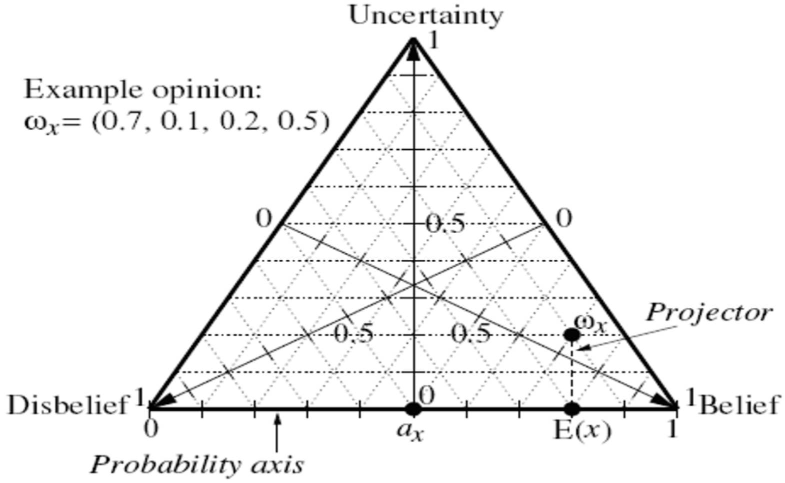

Figure 3 Opinion triangle with example opinion.

- A subject can write to an object only if the subject's SL is not higher than the object's SL.

MLS is applied in various fields including operating system, database management system, network, as well as transaction processing and web server. In sum, the advantages of MLS systems include five aspects as follows [21,22].

(1) It allows users at each SL to receive appropriate information.
(2) It protects data from malicious user.
(3) It processes data in secure and appropriate ways.
(4) It delivers data to the correct receiver without revealing any sensitive information.
(5) It improves system efficiency.

An example of multilevel secure routing is shown in Figure 4. Source *S* initiates a packet that is destined to *D* and its SL is Second. The packet will be transmitted following path 1, since only the mesh routers whose SLs are equal to or higher than the SL of the packet are allowed to participate in route discovery. On the other hand, if the packet is classified as Fourth, it will be sent through path 2, because the mesh routers on path 2 meet the security requirement with shorter distance. Therefore, packets transmission is not only secure, but also has various degrees of sensitivity. Hence, the scheme is able to provide communication that can handle the concept of security classifications.

4. The PA-SHWMP protocol

In this section, we present our privacy-aware secure routing protocol PA-SHWMP, which aims to provide privacy protection for WMNs. PA-SHWMP is based on the current draft version D3.02 [23] of IEEE 802.11s that introduces the concept of embedded routing in layer-2 named HWMP, which is a hybrid protocol because it has combined the flavor of reactive and proactive routing strategy by employing both on-demand path selection mode and proactive tree building mode. On-demand mode allows two MPs to communicate using peer-to-peer paths. On the other hand, proactive tree building mode can be an efficient choice for nodes in a fixed network topology. In HWMP, both on-demand and proactive modes can be used simultaneously. Figure 5[4] shows the principle of these two modes.

In PA-SHWMP, the user privacy information is divided into different categories according to the security requirements, which are diverse for different information to be transmitted under various circumstances, or with assorted available resources. Thus, it is able to provide balance between security and performance. To achieve the above purpose, a new field, SL as the indicator of security requirements, is added into the routing header to handle the security classifications for packets.

Routing process is to find the path from source to destination on which all the mesh routers meet the security requirements. Besides, to protect routing packets and user privacy information against attacks launched by the internal legitimate mesh routers, the protocol offers a subjective logic-based reputation mechanism for each mesh router to decide whether to provide services for incoming packets by querying the sender's reputation through their common neighbors and computing the expectation to estimate whether it is trustworthy or not.

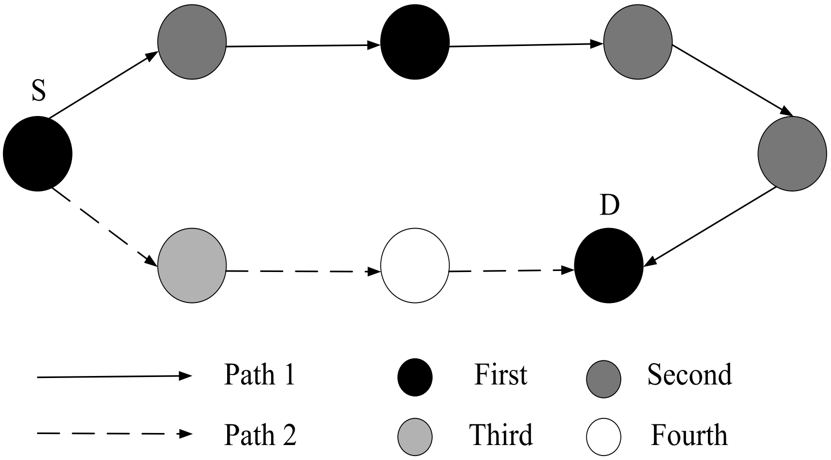

Figure 4 **An example of multilevel secure routing**.

The proposed scheme has made the following assumptions [22]:

1. All the packets exchanged through the network must have an SL which indicates the security requirements of the requested route.

2. All mesh routers must have an SL. The mesh router with a particular SL must only be allowed to transmit packets at the same level or a lower level.

3. The source may be any one of the participating mesh routers but can only send a packet with SL not higher than the SL of the source. This requirement can avoid bottleneck caused by mesh routers at lower SLs over-classify their packets with higher SL.

4. Each level is supplied with corresponding weight security services to assure the authenticity, integrity, and confidentiality of routing packets.

PA-SHWMP consists of the following three phases:

- security classification and reputation computation;
- packet authentication;
- routing confidentiality.

It is the combination of above mechanisms that provides expected security and efficiency during route discovery and maintenance. The details of PA-SHWMP are described next.

4.1. Subjective logic-based reputation scheme

In this article, we propose a novel reputation scheme which incorporates uncertainty-based subjective logic into the reputation computing. Also, in order to differentiate between intentional packet drop and packet drop

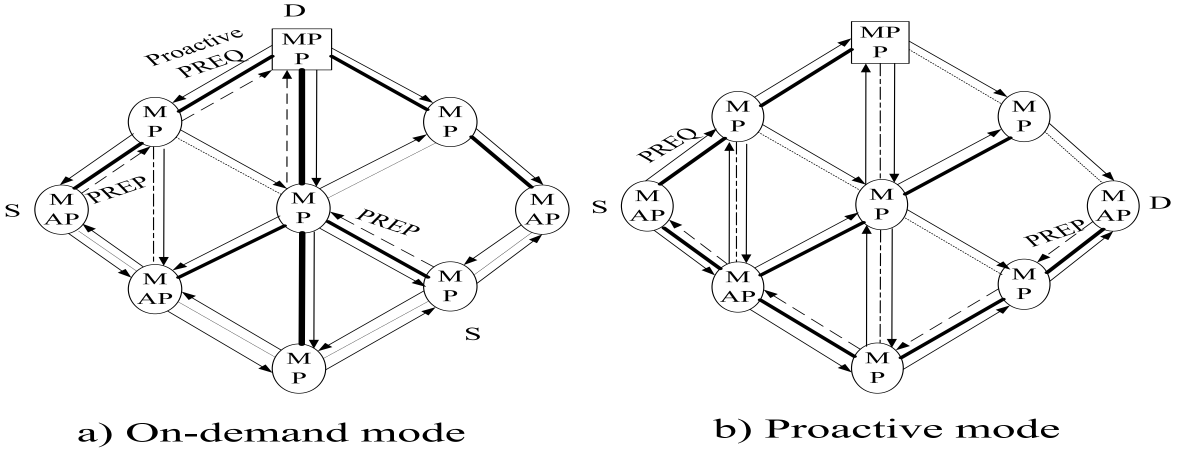

Figure 5 **Principle of HWMP** [4].

due to poor link quality, we integrate link quality into the proposed scheme.

The contributions of this novel reputation scheme are (1) it incorporates uncertainty-based subjective logic into the reputation computation, and detects the existing selfish and malicious mesh routers in the network. (2) It assigns the corresponding weight factor to each of the opinions from recommenders, which makes the final recommendation results more accurate. (3) It has a reconfirmation procedure for selfish and malicious mesh routers, which decreases the false positive rate and improves the network performance. (4) It makes use of link quality metric to differentiate between intentional packet drop and packet drop due to poor link quality.

(1) Quality of wireless links computation

In our scheme, we use the EAR [24] technique for estimating the quality of wireless links by the equation given as:

$$d_i = (1-\alpha) \times d_{i-1} + \alpha \times N_{\mathrm{s}}/N_{\mathrm{T}} \tag{2}$$

where d_i is the smoothed delivery ratio, α is the smoothed constant, $0 < \alpha < 1$, N_s is the number of successful transmissions during the measurement period of the ith cycle, N_{T} is the total number of transmissions during the measurement period of the ith cycle.

All the calculations in our scheme are performed in time domain. In order to facilitate the analysis and description, we do not announce it again in the following sections.

(2) Reputation computation

(1) Direct opinion

In WMNs, nodes x and y are two neighboring nodes, the final opinion of x to y $\omega_{x:y}^{\mathrm{final}}$ includes two components. One is the direct opinion $\omega_{x:y}^{\mathrm{dir}}$, the other is the testimonies from other nodes, e.g., the recommended opinions $\omega_{x:y}^{\mathrm{rec}}$.

The direct opinion of nodes x to y $\omega_{x:y}^{\mathrm{dir}} = (b_{x:y}^{\mathrm{dir}}, d_{x:y}^{\mathrm{dir}}, u_{x:y}^{\mathrm{dir}}, a_{x:y}^{\mathrm{dir}})$ is stored in x' local reputation table. Following the direct interaction history, node x computes $b_{x:y}^{\mathrm{dir}}$, $d_{x:y}^{\mathrm{dir}}$, and $u_{x:y}^{\mathrm{dir}}$. In a measurement period, we let $T_x(y)$ be the total number of packets node x has transmitted to node y for forwarding, $S_x(y)$ denotes the number of packets node y has successfully forwarded and $F_x(y)$ be the number of packets node y has not forwarded. The link quality between nodes x and y is $LQ(x, y)$, which can be calculated by (2). Then, we have the following equation:

$$\begin{cases} b_{x:y}^{\mathrm{dir}} = S_x(y)/(T_x(y) * LQ(x,y)) \\ d_{x:y}^{\mathrm{dir}} = F_x(y)/(T_x(y) * LQ(x,y)) \\ u_{x:y}^{\mathrm{dir}} = 1.0 - b_{x:y} - d_{x:y} \end{cases} \tag{3}$$

Each node has its direct opinion on others. For an entirely unknown node or a new node, the default opinion assigned by its neighbors is (0.0, 0.0, 1.0, a).

We classify interactions among nodes into positive interaction, negative interaction, and uncertain interaction. Each positive or negative interaction increases the rating of node's knowledge or decreases uncertainty. The parameter $\delta \in [0.0, 1.0]$ determines how much a rating change after an individual interaction between nodes. In the following formulae, we omit the subscript $x{:}y$ from each 4-tuple opinion. The direct opinions stored in node x's local reputation table are updated through the following formulae [7,8]:

This updated mechanism ensures that the direct opinion $\omega_{x:y}^{\mathrm{dir}} = (b_{x:y}^{\mathrm{dir}}, d_{x:y}^{\mathrm{dir}}, u_{x:y}^{\mathrm{dir}}, a_{x:y}^{\mathrm{dir}})$ can be updated in real time by providing a more precise $\omega_{x:y}^{\mathrm{dir}}$ for calculation of $\omega_{x:y}^{\mathrm{final}}$; meanwhile, with the increasing of the number of interactions, the uncertainty value will decrease to zero. All these can improve the accuracy of isolating untrustworthy nodes.

(2) Recommended opinions

When the direct opinion $\omega_{x:y}^{\mathrm{dir}}$ is not enough for node x to make a decision about node y, node x solicits the recommended opinions from their common neighbor nodes, the neighbor nodes transmit their direct opinions on node y as the recommended opinions to node x. Suppose that node x receives a number of n subjective opinions, known as recommended opinions. Let R represent the set of recommenders, for each recommender $i \in R$, we allocate an appropriate weight f_i to each recommended opinion. The weight f_i is computed as follows:

$$\begin{cases} f_i = E(\omega_{x:i}) \Big/ \sum_{k \in R} E(\omega_{x:k}) \\ E(\omega_{x:i}) = b_{x:i} + a_{x:i} u_{x:i} \end{cases} \tag{4}$$

Where $E(\omega_{x:i})$ represents x's belief on i. The larger $E(\omega_{x:i})$ will make bigger impact on the reputation computation result. For those untrustworthy nodes, their expectations are very small, so their recommending opinions will have little impacts on the reputation computation result, which prevents retaliations or badmouth from occurring after untrustworthy nodes are rejected.

Recall that the truster x may get recommendations about the trustee y from many different recommenders. Then, x's belief on the recommendation about y is the average of the belief values of all recommendations and x's disbelief is the average of the disbelief values of the recommendations. The same is true for x's uncertainty about the recommendations. Therefore, if there are a

(Continued)

If the interaction is a positive interaction,
If $u \geq \delta$, then

$$\begin{cases} b = b + \delta \\ u = u - \delta \end{cases}$$

Else

$$\begin{cases} b = b + \delta \\ d = d - (\delta - u) \\ u = 0.0 \end{cases}$$

If the interaction is a negative interaction,
If $u \geq \delta$, then

$$\begin{cases} d = d + \delta \\ u = u - \delta \end{cases}$$

Else

$$\begin{cases} b = b - (\delta - u) \\ d = d + \delta \\ u = 0.0 \end{cases}$$

If the interaction is an uncertain interaction,
If b, $d \geq \delta/2$, then

$$\begin{cases} b = b - \delta/2 \\ d = d - \delta/2 \\ u = u + \delta \end{cases}$$

Else if $b < \delta/2$ and $d \geq \delta/2$, then

$$\begin{cases} b = 0.0 \\ d = d - (\delta - b) \\ u = u + \delta \end{cases}$$

Else if $b \geq \delta/2$ and $d < \delta/2$, then

$$\begin{cases} b = b - (\delta - d) \\ d = 0.0 \\ u = u + \delta \end{cases}$$

Else if b, $d < \delta/2$, then

$$\begin{cases} b = 0.0 \\ d = 0.0 \\ u = 1.0 \end{cases}$$

group of n recommenders then the opinion $\omega_{x:y}^{\text{rec}} = (b_{x:y}^{\text{rec}}, d_{x:y}^{\text{rec}}, u_{x:y}^{\text{rec}}, a_{x:y}^{\text{rec}})$ is computed as

$$\begin{cases} b_{x:y}^{\text{rec}} = \sum_{k=1,k\in R}^{n} f_k \cdot b_{k:y}^{\text{dir}} \Big/ n \\ d_{x:y}^{\text{rec}} = \sum_{k=1,k\in R}^{n} f_k \cdot d_{k:y}^{\text{dir}} \Big/ n \\ u_{x:y}^{\text{rec}} = \sum_{k=1,k\in R}^{n} f_k \cdot u_{k:y}^{\text{dir}} \Big/ n \\ a_{x:y}^{\text{rec}} = \sum_{k=1,k\in R}^{n} f_k \cdot a_{k:y}^{\text{dir}} \Big/ n \end{cases} \tag{5}$$

(3) Final opinion

After getting the direct opinion $\omega_{x:y}^{\text{dir}}$ and the recommended opinion $\omega_{x:y}^{\text{rec}}$, a final opinion $\omega_{x:y}^{\text{final}} = (b_{x:y}^{\text{final}}, d_{x:y}^{\text{final}}, u_{x:y}^{\text{final}}, a_{x:y}^{\text{final}})$ is calculated as [8]

$$\begin{cases} b_{x:y}^{\text{final}} = \left(b_{x:y}^{\text{dir}} \cdot u_{x:y}^{\text{rec}} + b_{x:y}^{\text{rec}} \cdot u_{x:y}^{\text{dir}}\right) \Big/ \left(u_{x:y}^{\text{dir}} + u_{x:y}^{\text{rec}} - u_{x:y}^{\text{dir}} \cdot u_{x:y}^{\text{rec}}\right) \\ d_{x:y}^{\text{final}} = \left(d_{x:y}^{\text{dir}} \cdot u_{x:y}^{\text{rec}} + d_{x:y}^{\text{rec}} \cdot u_{x:y}^{\text{dir}}\right) \Big/ \left(u_{x:y}^{\text{dir}} + u_{x:y}^{\text{rec}} - u_{x:y}^{\text{dir}} \cdot u_{x:y}^{\text{rec}}\right) \\ u_{x:y}^{\text{final}} = \left(u_{x:y}^{\text{dir}} \cdot u_{x:y}^{\text{rec}}\right) \Big/ \left(u_{x:y}^{\text{dir}} + u_{x:y}^{\text{rec}} - u_{x:y}^{\text{dir}} \cdot u_{x:y}^{\text{rec}}\right) \\ a_{x:y}^{\text{final}} = a \end{cases} \tag{6}$$

When both the direct opinion $\omega_{x:y}^{\text{dir}}$ and the recommended opinion $\omega_{x:y}^{\text{rec}}$ are determined, and the denominator $(u_{x:y}^{\text{dir}} + u_{x:y}^{\text{rec}} - u_{x:y}^{\text{dir}} \cdot u_{x:y}^{\text{rec}})$ in (6) is zero, we compute the final opinion $\omega_{x:y}^{\text{final}}$ by (7)

$$\begin{cases} b_{x:y}^{\text{final}} = \beta \cdot b_{x:y}^{\text{dir}} + (1 - \beta) \cdot b_{x:y}^{\text{rec}} \\ d_{x:y}^{\text{final}} = \beta \cdot d_{x:y}^{\text{dir}} + (1 - \beta) \cdot d_{x:y}^{\text{rec}} \\ u_{x:y}^{\text{final}} = 0 \\ a_{x:y}^{\text{final}} = a \end{cases} \tag{7}$$

where β is a weight, which determines how much the direct opinion $\omega_{x:y}^{\text{dir}}$ impacts on the final opinion $\omega_{x:y}^{\text{final}}$.

4.2. Initialization

In PA-SHWMP, a trusted identity manager is pre-loaded, while every participating mesh router pre-loads an identity table. The identity table provides information about peering mesh routers in the network. Each entry of the table describes the identity of a specific mesh router by binding the following information together with the mesh router: IP address, SL, public key, and valid time period. Moreover, the mesh routers at higher SL have keys related to its own level and all the lower levels. The trusted identity manager has to reflect the current bindings of mesh routers in the WMNs, and mesh routers need to contact the identity manager when the service is available to keep the freshness and correctness of the identity table. Also, according to aforementioned assumptions, each mesh router participating in the protocol must be assigned a certain SL based on its hierarchic ranking or the role it plays in WMNs.

Appropriate mechanisms should be applied to guarantee the secure communications between mesh routers and the security manager. However, it is not our concern in this article.

4.3. Path selection

Prior to communicate with another mesh router in the network, the source constructs a message and labels it with an SL which indicates the security requirements on the requested route. The protocol checks whether the SL satisfies the condition of assumption 3. If not, the source must modify the SL and broadcast a PREQ (*path request)* packet to its neighbors.

Then, when a mesh router y requests one of its neighbors x for some service, the proposed novel reputation scheme is carried out to decide whether to provide the service. Let $\gamma \in$ [0.0, 1.0] be a threshold, if the expectation $E(\omega_{x:y})$ is larger than γ, y will be considered as a cooperative mesh router and the service request will be granted by x. The detail of the decision mechanism is described as follows.

1. y sends a Path_Request message to one of its neighbors x.
2. After receiving Path_Request successfully, x performs different formulae according to its type. If x is trustworthy, it performs formula (I); if x is untrustworthy, it performs formula (II).
Formula (I):
    (1) x retrieves its direct opinion $\omega_{x:y}^{\mathrm{dir}}$ from its local reputation table and calculates the expectation $E(\omega_{x:y}^{\mathrm{dir}})$.
    (2) If $E(\omega_{x:y}^{\mathrm{dir}}) \geq \gamma$, x sends an *Accept* message to y and provides the requested service, and y records a positive interaction with x; else, x invokes the reputation query procedure.
    (a) x broadcasts a *Reputation_Query* to the common neighbor nodes with y for the their recommending opinions on y and waits for a time interval T.
    (b) Any node k whose uncertainty $u_{k:y}^{\mathrm{dir}}$ of its direct opinion is less than 1.0 sends its direct opinion $\omega_{k:y}^{\mathrm{dir}}$ to x.
    (c) After the time interval T, x weights each received recommended opinions using (4), integrates them into a recommended opinion $\omega_{x:y}^{\mathrm{rec}}$ using (5), and combines the direct opinion $\omega_{x:y}^{\mathrm{dir}}$ with the recommended opinion $\omega_{x:y}^{\mathrm{rec}}$ using (6) or (7). Finally, x obtains the final opinion $\omega_{x:y}^{\mathrm{final}}$.
    (d) After obtaining the final opinion $\omega_{x:y}^{\mathrm{final}}$, x calculates its expectation $E(\omega_{x:y}^{\mathrm{final}})$. If $E(\omega_{x:y}^{\mathrm{final}}) \geq \gamma$, x sends an *Accept* message to y and provides the requested service, and y records a positive interaction with x; otherwise, x sends a *Refuse* message to y, and y records a negative interaction with x.
Formula (II):

Let $\theta \in$ [0.0, 1.0] be the probability that an untrustworthy mesh router cooperates in an attempt to hide its untrustworthy intent. When x receives a request message from y, then x flips a coin weighted by probability θ.

    (a) If the coin flip indicates to cooperate, x sends an *Accept* message to y and provides the requested service, and y records a positive interaction with x.
    (b) If the coin flip indicates not to cooperate, x refuses to provide service to y, and y records a negative interaction with x.
3. If the expectation of a mesh router y, $E(\omega_y) < \gamma$, y is perceived as untrustworthy. It is temporarily excluded from the network so that it is put into a probation state and can be forced to cooperate. Initially the probation period is T, which is the same as the period of reputation query. At the end of T, y is given another chance to calculate its expectation $E(\omega_y)$, if $E(\omega_y)$ is still less than γ, then y is put into another probation state for a longer period ($2T$). Therefore, the probation period of an untrustworthy mesh router is doubled on every subsequent offence until it reaches a maximum value $T_{\max}$, then it is permanently excluded from the network.

So far, the overall workflow of our proposed scheme is completed. Untrustworthy wireless mesh routers in WMNs are detected and isolated.

Finally, the intermediate trustworthy mesh routers compare the value of SL from received PREQ with their own SL's. If the SL of an intermediate mesh router does not meet the requirements of the SL in the original PREQ, it cannot participate in the route discovery and has to drop the PREQ. In other words, only mesh routers with higher SL can be used as a relay mesh router by mesh routers with lower SL, but not vise versa. Each mesh router can only retrieve parts of users' private information within the limit of its own SL. Without being exposed the entire user's identity when nonessential information is disclosed, the security of a user will not be threatened. The user remains a certain level of anonymity and keeps its private information under the umbrella. For example, if a package has a lowest security requirement RESTRITED on a route, then any mesh router in the WMNs has the qualification to participate in the route discovery. In such situation, the path with the shortest distance will be selected. If a package's security requirement is SECRET, then only the mesh routers with higher SL such as SECRET or TOP SECRET are allowed to relay it. When the PREQ reaches the destination, the destination sends a PREP back to the mesh router from which it received the PREQ. The mesh router forwards the PREP packet, also establishes a routing table entry for the destination, with the offered route security associated.

With the MLS and uncertainty-based subjective logic mechanisms PA-SHWMP is able to send packets with various sensitivities via paths that implement corresponding security guarantees. However, in order to enforce the protocol working as designed and protect the network against certain vulnerabilities, the link security authentication mechanism is also needed.

In PA-SHWMP, Merkle Tree [22] is used to implement the link security by securing the mutable fields that can be modified in the intermediate routers. Considering the scenario that a source *S* wants to communicate with a destination *X* as shown in Figure 6, the secure path selection process is carried out as Equations (1)-(15) in [4].

As described in [4], the secure path selection process includes on-demand and proactive modes. In the on-demand mode, *S* first creates a Merkle tree whose leaves are the hash of mutable fields of PREQ message and a MAC on the root of the Merkle tree using the GTK. Then, it broadcasts PREQ. Upon receiving the PREQ, any neighbor mesh router authenticates the mutable fields by hashing the values received in an ordered way, creates a MAC on it using the shared GTK and compares with the received MAC value of the root. If the two values match, the mesh router, where the PREQ is from, is authenticated. Finally, the mesh routers update the mutable fields and create Merkle trees from the modified fields. They also decrypt the non-mutable part and re-encrypt it with their own broadcast key and broadcast it following the same rules. After authenticating and receiving the PREQ, the destination updates the mutable fields, creates Merkle Tree, and unicasts a PREP message using the same principle with PTK in the reverse path.

In the Proactive RANN mode, the broadcast message RANN uses GTK to protect the non-mutable fields and authenticate the mutable fields. After receiving the RANN message, the MP that needs to setup a path to the root MP unicasts a PREQ to the root MP. On receiving each PREQ, the root MP replies with a PREP.

5. Security analysis

The security of the proposed routing protocol is based on the subjective logic and MLS technology. The subjective logic-based reputation mechanism makes use of querying the sender's reputation through their common neighbors and computing the expectation to decide whether to provide services for incoming packets while keeping the user privacy. On the other hand, the MLS divides the user privacy information into different categories according to the security requirements. The mesh router with a particular SL must only be allowed to transmit packets and get user privacy information at the same level or a lower level. Therefore, it delivers data to

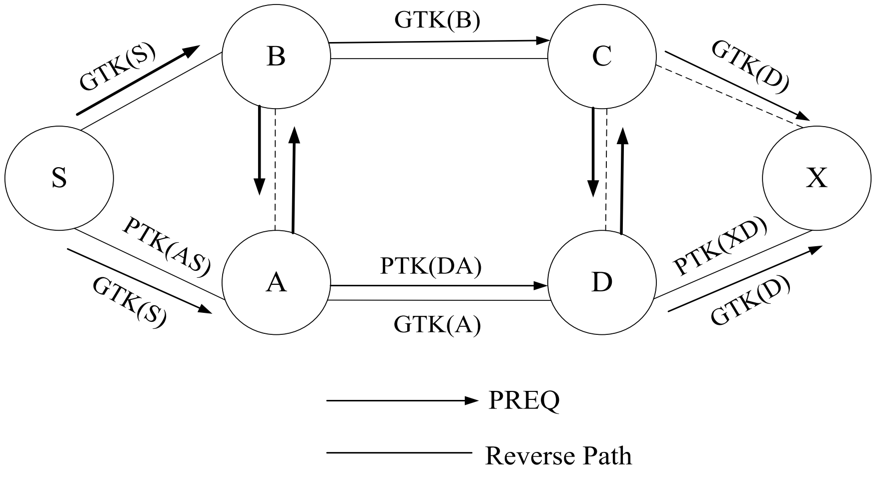

Figure 6 Secure path selection.

the correct receiver without revealing any sensitive information.

Equipped with protection features, the route messages as well as the user privacy information are protected from insiders. Packets and privacy information can only be recognized by legitimate mesh routers and opened by the expected destination mesh router.

In the following, we will discuss the security features of our protocols, including Route disruption and diversion attack, flooding attack, and impersonation attack.

Route disruption and diversion attack: route disruption and diversion attack aims to prevent discovering route between two legitimate mesh routers or divert traffic to malicious mesh routers by modifying the mutable fields in routing messages. A malicious mesh router can modify the metric field value to zero on the PREQ message and re-broadcast it. After receiving the modified PREQ, the destination mesh router will choose the malicious mesh router as the next hop in the reverse path and unicast PREP to the malicious mesh router. In this occasion, the malicious mesh router can disrupt the route discovery by dropping the valid PREP message destined for the source mesh router and all traffic to the destination mesh router will be diverted through the attacker. In PA-SHWMP, mutable fields in the routing information are authenticated in each hop, and only mesh routers that meet the security requirement embedded in the packets can participate in the route discovery phase. If there is any malicious modification on the value of a mutable field, it will be readily detected by the next hop by comparing the new MAC with the received one and the modified packet will be discarded. Also by encrypting certain fields at higher SL, read-up violation at the malicious mesh routers with lower SL can be prevented from interpreting the packets without higher-level key. With these methods, it is impossible to launch a route disruption and diversion attack that caused by the malicious behavior of a mesh router through modification of a mutable field and dropping routing information.

Flooding attack: Flooding attack aims to consume the network bandwidth and degrade the overall throughput by flooding the network with PREQ messages destined to an address which is not present in the network. In the sequel, intermediate mesh routers rebroadcast PREQ and within a short time the network is flooded with fake requests. In PA-SHWMP, participants only accept packets processed by a mesh router which meets the security requirement and is considered to be trustworthy. Moreover, the packets are signed with a private key or a group key. Therefore, a malicious mesh router cannot participate in the routing process or initiate a route discovery process with a destination address that is not in the network. Again, as the routing information is encrypted during transmission, a malicious mesh router cannot insert a new destination address.

Impersonation attack: Only inside attackers can do impersonation attack. If a mesh router is compromised, the attacker can use the compromised privacy information to masquerade as any other mesh client. In PA-SHWMP, only the source and destination can sign with its own private key, routers cannot spoof other routers in route instantiation and ensure that only the destination can respond to route discovery. This prevents either the source or the destination from spoofing.

6. Performance analysis

A typical WMN is characterized by low-power mobile devices and low-bandwidth wireless channels. The performance of routing protocols has a great impact on the applicability and usability of a WMN. We implement the PA-SHWMP in OPNET [25,26] and evaluate its performance by comparing it with the SHWMP and HWMP routing protocols. According to the scenario defined in [4,22], the network scenario parameters used in our simulation are listed in Table 2. In the simulation scenario, a mesh network of size 1000 × 1000 m^2 consists of 50 wireless mesh routers that are deployed randomly over the defined field. The mobile nodes are moving in the field according to the random waypoint model [26], and their average speeds range from 0 to 2 m/s. An omni-directional constant bit-rate (CBR) traffic is generated for 5 to 10 random pairs to resemble point-to-point communication in the real world. All protocols are run under the identical traffic scenario.

We consider the following performance metrics:

- Packet delivery ratio (PDR): Ratio of the number of data packets received at the destinations to the number of data packets generated by the CBR sources. It in turn

Table 1 Simulation parameters

Parameter	Value
Traffic type	CBR
Simulation area	1000 × 1000 m^2
Packet rate	2 packets/s
Total number of wireless nodes	50
Maximum number of malicious nodes	25
Simulation time	900 s
Packet size	1024/512 bytes
Base rate a	0.5
Variation δ	0.1
Weight factor β	0.5
Maximum cooperation rate of selfish nodes θ	0.3
Threshold γ	0.6
Reputation query period T	5 s
Isolation time $T_{\max}$	20 s

determines the efficiency of the protocol to discover routes successfully.

- Path acquisition delay: Time required to establish a route from source to destination which actually measures the delay between sending a PREQ/proactive PREQ to a destination and the receipt of corresponding PREP.
- End-to-end delay: Average delay experienced by a data packet from a source to destination. Note that, end-to-end delay includes all the delays including medium access delay, processing delays at intermediate mesh routers, etc.
- False positive rate: It is defined as the percentage of number of cooperative mesh routers wrongly detected as selfish or malicious out of the total number of cooperative mesh routers in the network. It is desirable for this rate to be as small as possible.
- Convergence time: Another factor of interest is convergence time, which is the time for cooperative wireless mesh routers to detect and throttle selfish or malicious wireless mesh routers completely. It is desirable for this time to be as small as possible.

Simulations have been run over ten times with random seeds. The performance metrics used in our proposed scheme are then collected and averaged. To ensure a valid comparison, the sequence of random seeds is the same and the only variation is the choice of parameters.

We first evaluate the performance of detecting malicious routers by measuring the PDR. Figure 7 shows the average PDR of PA-SHWMP compared with SHWMP and HWMP with different numbers of malicious routers. As depicted in Figure 7, the performance of network decreases as the number of malicious routers increases. When there are no malicious routers in the network, the PDR of PA-SHWMP is slightly lower than SHWMP and HWMP due to the detection overhead. As the number of malicious routers increases, the PDR of PA-SHWMP decreases more slowly than that of SHWMP and HWMP attributed to more accurate node isolation due to the reconfirmation procedure. It should be noted that when the number of malicious routers increases beyond 15, the performance improvement shown by the detection scheme starts to decline. The difference between the three protocols becomes smaller and smaller. The reason is that the higher the ratio of malicious routers, the more legitimate mesh routers are left unreachable from the mesh gateway and the fewer alternatives are available for choosing forwarding paths.

Figures 8 and 9 compare the average end-to-end delay and average path acquisition delay of the three protocols. We run the simulation using five and ten source-destination pairs. As shown in Figures 8 and 9, under light or medium traffic loads and less hops, the delay is less than 200 ms, whereas under heavy traffic loads and more hops, the delay reaches to nearly 300 ms. Furthermore, both the end-to-end delay and the average path acquisition delay of PA-SHWMP are much higher than SHWMP and HWMP. The lower performance of the PA-SHWMP is due to two facts: (1) Heavy traffic loads result in more frequent and serious congestion and signal interference in the network. Packets get lost or dropped more easily. (2) More hops results in more processing time for computing the values of reputation and SL as well as doing the link security authentication to verify the authenticity of a received packet.

Figure 10 illustrates the effect of poor quality links on performance by simulating some wireless links in the network to perform poorly, which could happen in real life due to wireless network characteristics. The

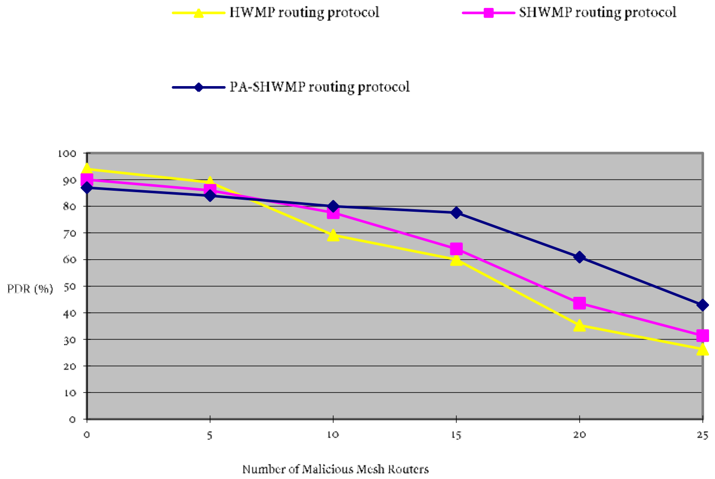

Figure 7 PDR comparison in the presence of malicious mesh routers.

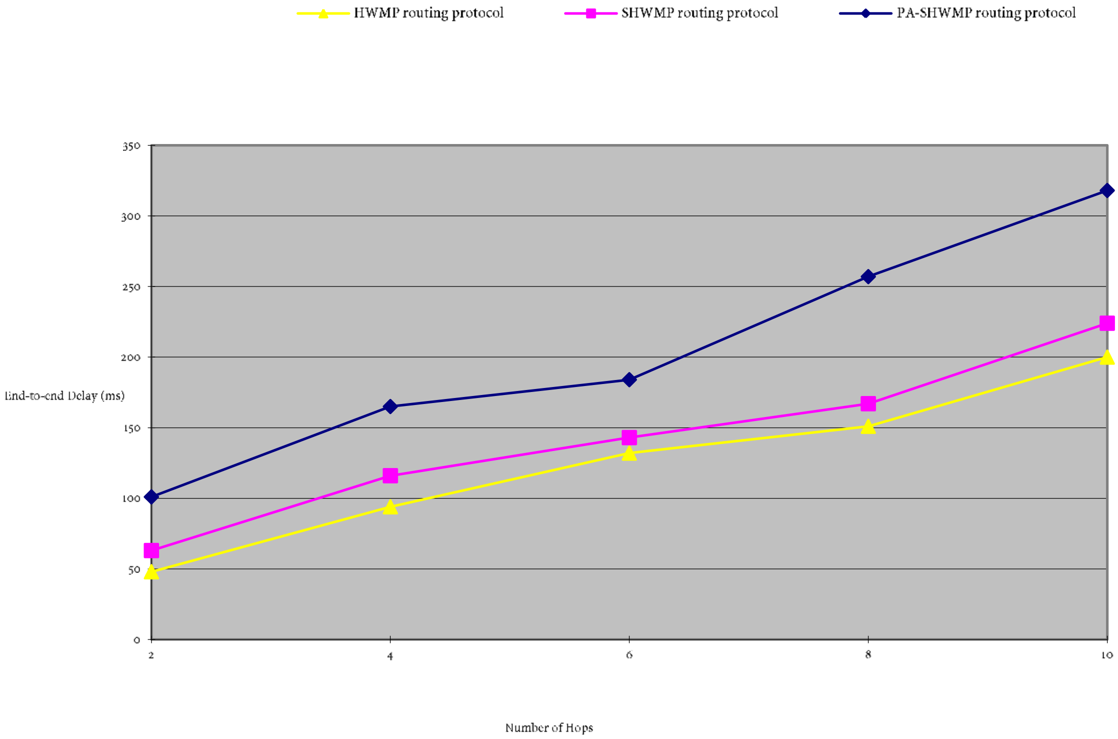

Figure 8 Average end-to-end delay.

forwarding ratio of the poor quality links ranges from 0.4 to 0.6. In the simulation, we varied the number of lossy wireless links and examined the number of false positives that can be explained by the packet loss caused by congestions. From the simulation results, we can see that when the number of lossy links increases, the false positive rates of both SHWMP and HWMP increase, while the false positive rate of PA-SHWMP decreases.

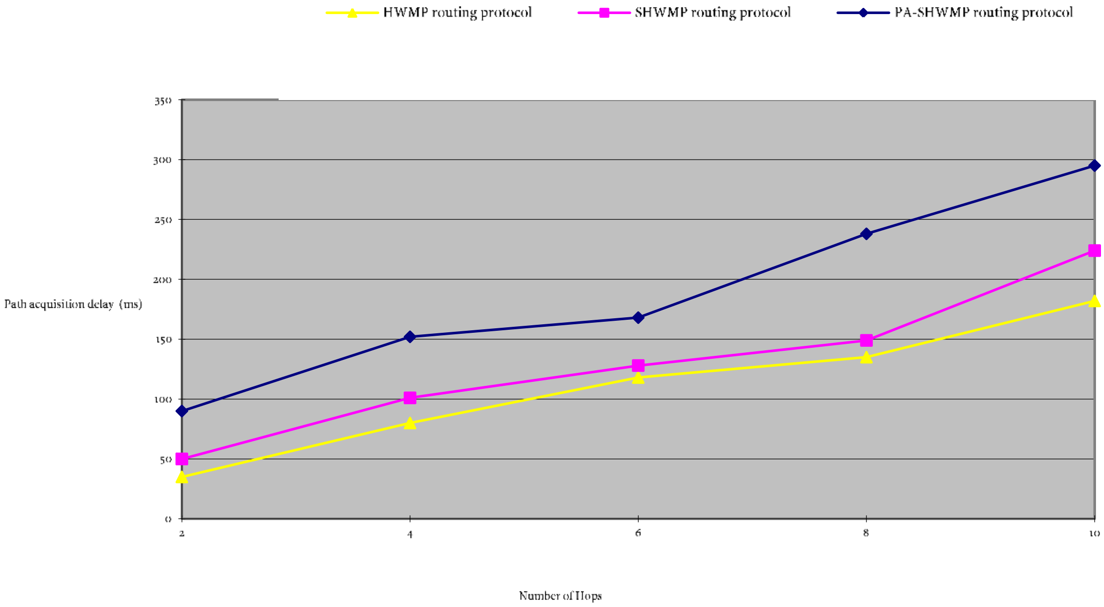

Figure 9 Average path acquisition delay.

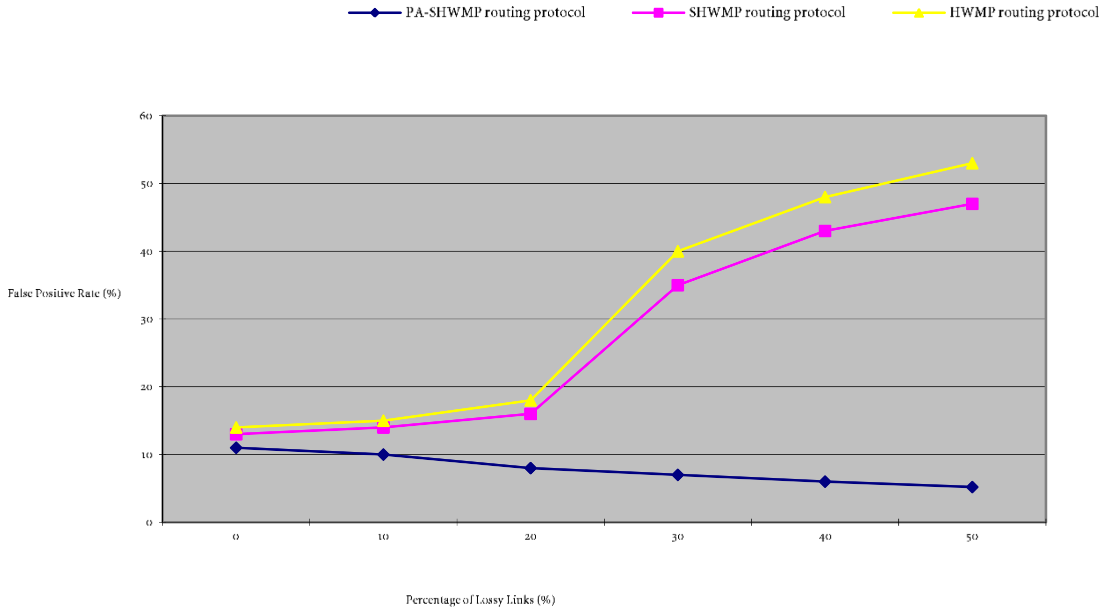

Figure 10 Comparison of false positive rate as a function of link quality.

The reason is that poor quality link causes a lot of packets loss, neither SHWMP nor HWMP has mechanisms to differentiate between intentional packet drops and packet drops due to link quality, thus their packet losses due to link quality are falsely detected as misbehavior, which increases their false positive rates. On the contrary, PA-SHWMP can effectively differentiate the packet losses due to link quality.

Figure 11 compares the three protocols in terms of PDR. As shown in Figure 11, with the increase in the percentage of lossy links, the PDR values of the three protocols decrease and the decrease of PA-SHWMP is smoother than the other two protocols. The reason is that both SHWMP and HWMP falsely detect certain mesh routers as malicious due to their poor wireless links, with the increase in the percentage of lossy links, an increasing number of legitimate mesh routers are excluded from the network, which results in a rapidly decreasing PDR for both SHWMP and HWMP.

Finally, we compare the convergence time used to isolate malicious mesh routers. In the simulation, the parameter θ is set to be 0.3; so, malicious mesh routers can hide their misbehaviors to a certain degree. As we can observe from Figure 12, convergence times of the three

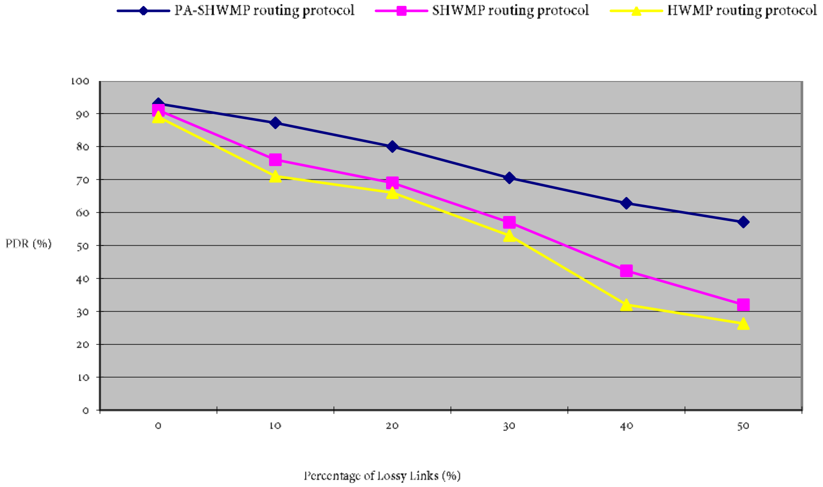

Figure 11 Comparison of PDR as a function of link quality.

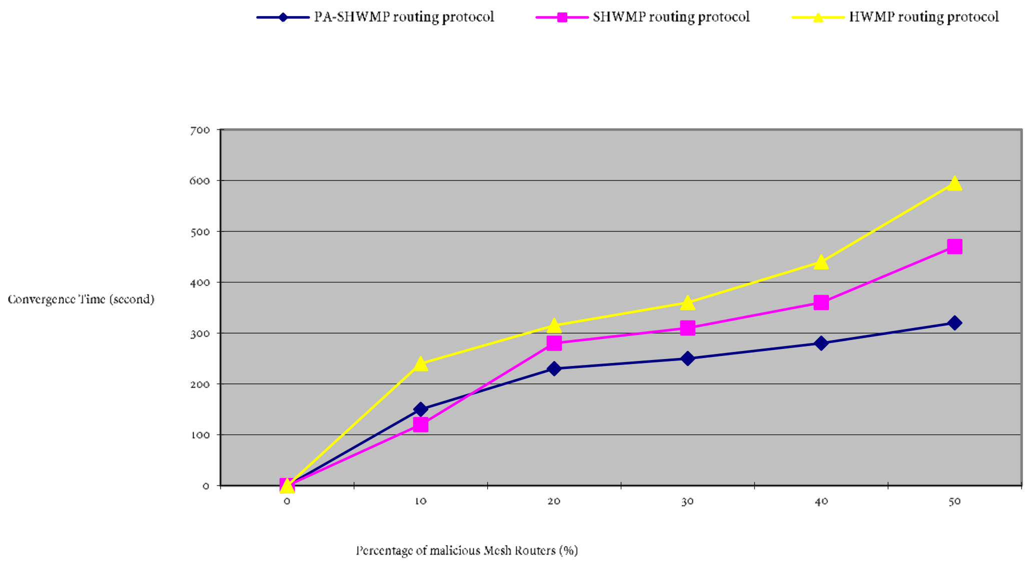

Figure 12 Comparison of convergent time as a function of link quality.

protocols raise as the percentage of malicious mesh routers increases. Moreover, convergence time of PA-SHWMP is smaller than the other two protocols under any specific percentage of malicious mesh routers. As the percentage of malicious mesh routers increases, the reliable information used for calculating the reputation values becomes less, causing the isolation of more malicious mesh routers, which leads to more broken forwarding routings. Thus, cooperative mesh routers have to spend more time to discover other malicious mesh routers. Due to the introduction of weight factor *f* and the reconfirmation scheme of malicious mesh routers, the proposed PA-SHWMP scheme can calculate reputation values and isolate malicious mesh routers more accurately. As a result, its convergence time also has a large improvement as shown in Figure 12.

7. Conclusions

In this article, we have investigated the problem of privacy preserving routing in WMNs and proposed a routing protocol, called PA-SHWMP to provide privacy protection and security in WMNs. PA-SHWMP is based on subjective logic and MLS technology and consists of three phases: (1) security classification and reputation computation; (2) packet authentication; (3) routing confidentiality. Relying on the hybrid usage of reputation mechanism and user privacy information classification mechanism, PA-SHWMP can provide scalable security services to assure the authenticity, integrity, and secrecy of routing packets and defend against the internal attacks caused by compromised mesh routers. Detailed security analysis and performance evaluation demonstrate that the proposed PA-SHWMP is secure, privacy preserving, and efficient. More specifically, the simulation results show that the PDR of the proposed PA-SHWMP becomes better than that of the existing HWMP and SHWMP protocols, when the number of malicious nodes and the percentage of lossy links increase. In addition, the convergence time of PA-SHWMP is smaller than HWMP and SHWMP with any percentage of malicious mesh routers.

Acknowledgements

The authors would like to thank the anonymous reviewers and the editor for their constructive comments that have helped us to improve this article. This study was supported by the Key Program of NSFC-Guangdong Union Foundation (U1135002), Major national S&T program (2011ZX03005-002), the National Natural Science Foundation of China (60872041, 61072080, 61072066), and the Fundamental Research Funds for the Central Universities (JY10000903001).

Author details

[1]School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, 710071 China [2]Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou, 350007 China [3]Department of Computer Science, Liverpool Hope University, L16 9JD, UK

Competing interests

The authors declare that they have no competing interests.

Received: 2 April 2011 Accepted: 28 February 2012
Published: 28 February 2012

References

1. IF Akyildiz, X Wang, W Wang, Wireless mesh networks: a survey. Comput Netw. **47**(4), 445–487 (2005). doi:10.1016/j.comnet.2004.12.001
2. W Lou, K Ren, Security, privacy, and accountability in wireless access networks. IEEE Wirel Commun Mag. **16**, 80–87 (2009)
3. Z Wan, K Ren, B Zhu, B Preneel, M Gu, Anonymous user communication for privacy protection in wireless metropolitan mesh networks. IEEE Trans Veh Technol. **59**(2), 519–532 (2010)

4. MS Islam, MA Hamid, CS Hong, SHWMP: a secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks. Trans Comput Sci VI. **5730**, 95–114 (2009). doi:10.1007/978-3-642-10649-1_6
5. N Li, N Zhang, SK Das, B Thuraisingham, Privacy preservation in wireless sensor networks: a state-of-the-art survey. Ad Hoc Netw. **7**, 1501–1514 (2009). doi:10.1016/j.adhoc.2009.04.009
6. S Khan, KK Loo, N Mast, T Naeem, SRPM: secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks. Netw Syst Manag. **18**(2), 190–209 (2010). doi:10.1007/s10922-009-9143-3
7. P Kane, PC Browne, Using uncertainty in reputation methods to enforce cooperation in ad-hoc networks, in *Proc of the 5th ACM Workshop on Wireless Security*, New York, NY, USA, 105–113 (Sept 2006)
8. 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 Comput Syst. **27**(5), 547–554 (2011). doi:10.1016/j.future.2010.03.006
9. F Li, J Wu, Uncertainty modeling and reduction in MANETs. IEEE Trans Mob Comput. **9**(7), 1035–1048 (2010)
10. http://www.disa.mil
11. H Li, AP Dhawan, Mosar: a secured on-demand routing protocol for mobile multilevel ad hoc. Int J Netw Secur. **10**(2), 121–134 (2010)
12. C Li, Z Wang, C Yang, Secure routing for wireless mesh networks. Int J Netw Secur. **13**(2), 109–120 (2011)
13. S Capkun, J Hubaux, M Jakobsson, Secure and privacy preserving communication in hybrid ad hoc networks. EPFL-IC Technical report IC/2004/10 (January 2004)
14. X Wu, N Li, Achieving privacy in mesh networks, in *Proc of the fourth ACM Workshop on Security of Ad hoc and Sensor Networks (SASN'06)*, New York, NY, USA, 13–22 (October 2006)
15. T Wu, Y Xue, Y Chi, Preserving traffic privacy in wireless mesh networks, in *Proc of International Symposium WoWMoM*, Washington, DC, USA, 449–461 (June 2006)
16. F Samad, SA Makram, Protection based on neighborhood-trust in clustered wireless mesh networks, in *Proc of Third International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST)*, Cardiff, Wales, UK, 487–493 (Sept 2009)
17. K Ren, S Yu, W Lou, Y Zhang, PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks. IEEE Trans Parallel Distrib Syst. **21**(2), 203–215 (2010)
18. J Sen, An efficient and user privacy-preserving routing protocol for wireless mesh networks. Int J Scalable Comput Practice Exp. **11**(4), 345–358 (2011). (Special Issue on Network and Distributed Systems)
19. A Jøsang, R Hayward, S Pope, Trust network analysis with subjective logic. in *Proc of the 29th Australasian Computer Science Conference*, CRPIT Volume 48, Hobart, Australia, 85–94 (January 2006)
20. G Shafer, *A Mathematical Theory of Evidence* (Princeton University Press, Princeton, NJ, 1976)
21. W-P Lu, MK Sundareshan, A model for multilevel security in computer networks. IEEE Trans Softw Eng. **16**(6), 647–659 (1990). doi:10.1109/32.55093
22. MS Islam, YJ Yoon, MA Hamid, CS Hong, A secure hybrid wireless mesh protocol for 802.11s mesh network. in *Proc of ICCSA 2008*, LNCS 5072, Davis, CA, 972–985 (June 2008)
23. IEEE 802.11s Task Group, Draft Amendment to Standard for Information Technology Telecommunications and Information Exchange Between Systems–LAN/MAN Specific Requirements–Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE P802.11s/D3.02 (May 2009)
24. K Kim, KG Shin, On accurate measurement of link quality in multi-hop wireless mesh networks, in *Proc of the 12th Annual International Conference on Mobile Computing and Networking (MobiCom'06)*, Los Angeles, CA, USA, 38–49 (September 2006)
25. M Chen, *OPNET Network Simulation* (Beijing Tsinghua University Press, China, 2004)
26. DB Johnson, DA Maltz, Dynamic source routing in ad hoc wireless networks. Mob Comput. **353**, 153–181 (1996). doi:10.1007/978-0-585-29603-6_5

doi:10.1186/1687-1499-2012-69
Cite this article as: Lin *et al.*: PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks. *EURASIP Journal on Wireless Communications and Networking* 2012 **2012**:69.