FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs

Qiang Liu, Jianping Yin, Victor C. M. Leung, *Fellow, IEEE,* and Zhiping Cai, *Member, IEEE*

***Abstract*—Data security, which is concerned with the confidentiality, integrity and availability of data, is still challenging the application of wireless mesh networks (WMNs). In this paper, we focus on a special type of denial-of-service attack, called selective forwarding or grey hole attack. When this attack is launched at the gateways of a WMN where data tend to aggregate, it could lead to severe damages due to loss of sensitive data. Most existing proposals that focus on detecting stand-alone attackers via channel overhearing are ineffective against collusive attackers. In this paper, we propose a forwarding assessment based detection (FADE) scheme to mitigate collaborative grey hole attacks. Specifically, FADE detects sophisticated attacks by means of forwarding assessments aided by two-hop acknowledgement monitoring. Moreover, FADE can coexist with contemporary link security techniques. We analyze the optimal detection threshold that minimizes the sum of false positive rate and false negative rate of FADE, considering the network dynamics due to degraded channel quality or medium access collisions. Extensive simulation results are presented to demonstrate the adaptability of FADE to network dynamics and its effectiveness in detecting collaborative grey hole attacks.**

***Index Terms*—Wireless mesh network, collaborative grey hole attack, two-hop acknowledgement, forwarding assessment based detection, optimal detection thresholds**

I. Introduction

WIRELESS mesh network (WMN) [1] has recently emerged as a promising technology to provide better services to user terminals for applications such as community networking, ubiquitous wireless broadband Internet access, etc. In 2012, IEEE released an up-to-date version of the IEEE 802.11 Standard [2] including a specification of mesh networking. However, WMNs are susceptible to security issues due to its shared medium, multi-hop relay, lack of physical protection and aggregated traffic. Similar to wireless sensor networks (WSNs), WMNs are multi-hop networks. Thus, they are vulnerable to various routing protocol attacks, such selective forwarding [3], blackhole [4], wormhole [5] and sinkhole [6] attacks.

In this paper, we investigate the selective forwarding attack, also known as the grey hole attack, due to its serious threats to some data-sensitive applications such as heath-care monitoring and fire monitoring. Specifically, the motivation of selecting this attack for studies stems from two points: 1) Smarter and more powerful mobile devices are promoting the development and deployment of data-centric mobile applications. Emerging WMNs enable mobile terminals to access critical services over the global communication infrastructure anytime and anywhere. Thus, providing secure and reliable data delivery in this environment is an important requirement. 2) In WMNs, wireless mesh routers (MRs) are vulnerable to be captured by attackers due to software vulnerabilities in mobile operating systems and lack of physical protection. A compromised, malicious router can silently discard data packets to degrade the network performance. The difficulty of detecting the presence of such attacks in the presence of normal packet losses requires more in-depth studies in order to enable robust data delivery. In this attack, malicious nodes forward control packets normally but selectively drop data packets. The attack could lead to serious damage when sensitive data are lost. Moreover, since network traffic in a WMN aggregates at a special type of MR, called the gateway, which connects the mesh backbone with the global network. Thus, an attacker can advertise a route with the minimum cost to the gateway, then it can selectively drop data packets received from upstream MRs. While most of the existing studies on selective forwarding attacks [5] [7] [8] [9] focus on detecting stand-alone attackers based on channel overhearing, we examine a more sophisticated scenario in which multiple malicious nodes perform collaborative grey hole attacks. In addition, some security features like per-link encryption provided by [2] render existing detection solutions that rely on channel overhearing unusable. Therefore, it is important to develop novel methods that are compatible with contemporary link layer protection schemes. In this paper, we propose a forwarding assessment based detection (FADE) scheme to address the above two challenges.

The main contributions of this work are as follows:

1) We propose FADE, which combines downstream assessments and end-to-end assessments to detect sophisticated grey hole attacks. FADE uses fast hashing and digital signature techniques to protect packets against manipulation, replay and masquerading attacks at MRs. Besides, FADE is able to detect malicious accusation attack and counterfeit mark attack by examining the opinions of forwarding assessments. A two-hop acknowledgement mechanism is integrated with forwarding assessments to make FADE compatible with enhanced link

Manuscript received December 2, 2012; revised March 19, 2013 and June 25, 2013; accepted August 10, 2013. The associate editor coordinating the review of this letter and approving it for publication was N. Kato.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61170287, 60970034, 61232016 and 61070198).

Q. Liu is with the School of Computer, National University of Defense Technology, Changsha, Hunan, China. He is now a Visiting Scholar in the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada (e-mail: libra6032009@gmail.com).

J. Yin and Z. Cai are with the School of Computer, National University of Defense Technology, Changsha, Hunan, China (e-mail: {jpyin, zpcai}@nudt.edu.cn).

V. C. M. Leung is with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada (e-mail: vleung@ece.ubc.ca).

Digital Object Identifier xxx

layer security such as that specified in [2]. Therefore, the FADE scheme and link-by-link protection can coexist to reinforce the security of WMNs.

2) We perform a theoretical analysis to determine the optimal detection thresholds of FADE to minimize the sum of false positive and false negative rates, taking into account of normal packet losses due to poor channel quality and medium access collisions. Extensive simulations confirm our analysis and demonstrate that the detection thresholds can be effectively adjusted under varying network conditions.

The rest of this paper is organized as follows: The next section reviews the related work. Section III presents the system model and some assumptions. Section IV gives a detailed description of FADE. Section V analyzes the selection of detection thresholds in the presence of normal losses. Section VI presents extensive simulation results to illustrate the advantages of FADE. Section VII concludes the paper.

II. Related Work

In the past few years, motivated by the wide applications and security challenges of WSNs, many schemes to counter selective forwarding attacks in WSNs have been proposed, such as MDT [3], CHEMAS [10], LEDS [11] and UnMask [5]. Based on their functionalities, these schemes may be classified into four categories: 1) Attack detection schemes [4] [12]. Their goal is to detect the presence of selective forwarding attacks. However, they are not able to or concerned with locating the attackers. Complementary restoration schemes should be used with these identification schemes to eliminate the impacts of such attacks. 2) Malicious node detection schemes. They aim at identifying malicious nodes. Basically, these schemes require complex countermeasures to achieve the goal, such as incremental hash authentication scheme [13], location binding, checkpoint selection [10], and network flow analysis [6]. 3) Robustness reinforcement methods. These methods mainly focus on enhancing reliability of data delivery under selective forwarding attacks. There are two promising techniques that involve introducing redundancy [3] [11] or uncertainty [10]. 4) Attack resilient protocols [5] [14] [15] [16]. A notable characteristic of these protocols is that security and resiliency to attacks are considered in the design phase. The resilient protocols are intrinsically capable of defeating attacks because secure routing and key management are both considered in most cases. However, they are also complex and resource consuming, thus attack resilient protocols should be carefully designed in order to trade-off security with efficiency. Due to the nature of strategic interactions between malicious nodes and intrusion detectors, game theoretic approaches [17] have been studied to optimize the defense against selective forwarding attacks in WSNs, e.g., by selecting the route with the highest average utility value [18] and detecting malicious nodes using selected points on the forward path [19].

The channel aware detection (CAD) algorithm [9] differentiates selective forwarding misbehavior from normal losses caused by medium access collisions or poor channel quality based on channel estimation and traffic monitoring. If the monitored loss rate exceeds the estimated loss rate, those nodes are identified as grey hole attackers. One key disadvantage of CAD is that it fails to detect collusive attacks, which will be discussed in detail in the next section. Therefore, in [20] the authors extend CAD by proposing a channel appraisal method to detect colluding selective forwarding attacks. This method includes two phases: channel-aware detection and detection of colluding nodes. The first phase utilizes CAD to detect malicious behaviors, while the second phase further analyzes the suspicious nodes that are detected in the first phase to identify colluding nodes. However, the performance of this method depends highly on the effectiveness of CAD. Hence, if some sophisticated attacks evade detection by the CAD algorithm, then they will successfully evade detection by the method in [20] as well. Other traffic monitoring based detection methods can be found in [21] [22] [23] [24]. The methods in [23] [24] are robust against collaborative grey hole attacks. A hash function based method is proposed in [23] to generate node behavioral proofs that contain information from both received data packets and forwarding paths. The intermediate node uses a random number and the received packet to calculate the new proof of the packet and the forwarding path. Moreover, the authors proved some theorem to show that the hash based method could defend against collusive attacks. Many contemporary WMNs employ per-link encryption, as specified in [2], which makes overhearing based detection methods ineffective [25]. Thus, novel security solutions should be designed to work with the per-link security schemes.

In addition to traffic monitoring based methods, secure routing protocols for WMNs have also been studied extensively [8] [26] [27] [28] [29]. In [28], the authors proposed a source-routed, link-state, multi-path routing protocol with a probabilistic twist, called Sprout, which is resilient to attacks owing to probabilistic route generations and probabilistic route selections with route performance feedback. Based on the link-state graph constructed through a secure link-state dissemination protocol, the route generation phase quickly finds a highly diverse set of routes, then the route selection phase balances the exploration of new routes with the exploitation of known, active routes using route performance feedbacks to achieve a good tradeoff between security and performance under different attacks. However, it is possible that this method may select some polluted routes, with a higher probability in a network scenario with a lower route diversity. In addition, some robustness reinforcement methods, e.g., multi-path transmissions [29], public key infrastructure and quality of service guarantee [30], are also feasible for use in WMNs because MRs with multiple interfaces typically have higher processing, storage, and energy capacities.

III. System Model and Assumptions

A. Network Model

Generally speaking, WMN architectures can be classified into three groups according to the functionality and the mobility of the nodes, namely infrastructure based WMNs, client WMNs and hybrid WMNs [1]. In this paper, we consider a multi-interface infrastructure WMN, where stationary MRs

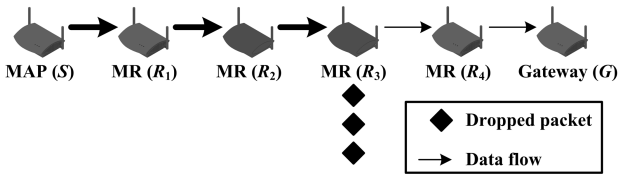


Fig. 1. Collaborative grey hole attack in a network with one source (S), one destination (G) and two malicious nodes (R_2 and R_3) that act in collusion.

form an infrastructure for mesh clients (MCs) to access mobile services. One or more MRs serve as gateways that aggregate traffic from MCs and relay network traffic between the WMN and the global Internet. On the other hand, all mobile MCs directly communicate with some mesh access points (MAPs). Thus the WMN can provide Internet connectivity as well as end-to-end communications for MCs via multi-hop packet transmissions over MRs.

B. Collaborative Attack Model

Since MRs are typically deployed outdoors without strong physical protection, an adversary may compromise some MRs through physical capture or software vulnerabilities and then have full control of these MRs. Afterwards, the adversary gains access to all sensitive data in the captured MRs such as group keys, public and private keys. Furthermore, the adversary can instruct the captured MRs to behave in a malicious manner, e.g., selectively dropping data packets. Most of the routing protocols designed for wireless multi-hop networks, e.g., Ad hoc On-Demand Distance Vector (AODV) [31] and Hybrid Wireless Mesh Protocol (HWMP) [2], assume that all nodes faithfully forward packets. Since these routing protocols aim to maintain network connectivity and a high network throughput, they are designed without self-contained security. The sinkhole attack [6] is a typical threat to these routing protocols. Malicious nodes that are present in the forwarding paths of data packets can launch selective forwarding attacks at any time. Several detection schemes and secure routing protocols have been proposed to identify or to bypass malicious nodes [9] [26]. However, they are not very effective against collaborative grey hole attacks, as demonstrated by the following example. In Fig. 1, a data flow originated from the source MAP S and terminated at the destination gateway G goes through a forwarding path with four intermediate MRs, namely R_1, R_2, R_3 and R_4. We assume that R_2 and R_3 are compromised MRs that act in collusion. It is possible that both R_2 and R_3 coexist on the forwarding path by advertising that the path including these two compromised nodes has the highest quality. The second attacker, i.e., R_3, is responsible for dropping data packets.

To clarify the attacking effects of collaborative grey hole attacks, two assumptions are made in our example: 1) Error-free wireless channel. Packets are dropped only due to the attacks; 2) No per-link encryption. Channel overhearing is possible. Taking CAD [9] as an example, we now demonstrate how the collaborative grey hole attack evades detection.

As indicated in [9], the kernel modules of CAD perform upstream and downstream traffic monitoring. They are the basis of attack detection and identification of compromised nodes. As mentioned above, the compromised node R_3 selectively drops data packets. On the other hand, the other malicious node R_2 pampers its partner R_3 and forges the result of downstream monitoring. To explain the collusive behaviors of R_2 and R_3, we denote $n_U(v_i, v_{i-1})$ and $n_D(v_i, v_{i+1})$, respectively, as the numbers of data packets received by v_i from v_{i-1} and dropped by v_{i+1} in a processing period. Moreover, $n_F(v_i)$ means the number of packets delivered to the downstream node. According to the definitions of opinions to the upstream and the downstream, the upstream opinion of R_i ($i \in \{1, 2, 3, 4\}$) is determined by comparing $(1 - n_U(R_i, R_{i-1})/n_U(R_{i-1}, R_{i-2}))$ with the upstream threshold, and the downstream opinion of R_i is calculated by comparing $n_D(R_i, R_{i+1})/n_F(R_i)$ with the downstream threshold. Because all nodes other than R_2 and R_3 behave normally, the upstream opinion of R_1, R_2 and the downstream opinion of R_3, R_4 must be normal. Since the malicious node R_2 does not drop packets, it is obvious that the downstream opinion of R_1 is normal too. While R_2 is supposed to monitor the dropping behavior of R_3, R_2 does not tell the truth because the two nodes are collusive. Thus, the downstream opinion of R_2 is normal regardless of high values of $n_D(R_2, R_3)/n_F(R_2)$. For the node R_3, the upstream opinion is still normal due to the fact that R_2 does not drop packets. Finally, we examine the upstream opinion of the normal node R_4. Since the node R_3 drops some packets, the value of $n_U(R_4, R_3)$ is in fact much smaller than that of $n_U(R_3, R_2)$. However, the node R_3 will tamper the value of $n_U(R_3, R_2)$ in order to dramatically decrease the value of $n_U(R_4, R_3)/n_U(R_3, R_2)$. Therefore, the upstream opinion of R_4 will still be normal. Then, the collaborative grey hole attack launched by R_2 and R_3 successfully evades CAD detection.

C. Assumptions

As we mentioned before, MRs in infrastructure WMNs form a mesh backbone for conventional MCs. Thus, we assume that all MRs are stationary and have enough processing and storage capacities as well as available power supply. Moreover, the inherent characteristics of WMNs, such as the broadcast nature of the radio transmission, the absence of an infrastructure, the multi-hop communications, the dynamical topology, and the decentralized and self-organizing nature make secure service a challenge. Therefore, there are extensive research efforts in key management and certificate management in wireless and mobile networks [30] [32]. Specifically, some practical solutions for key management were proposed to eliminate the key management centre and handle the dynamics, such as the multi-hop proxy encryption [33], the physical-layer-based key generation [34], secure clustering along with a pairwise key management based on public key cryptography [35]. On the other hand, the solutions for efficient public key certificate management in wireless and mobile networks were discussed in [32] [36]. To enhance the survivability of key management in the presence of different attacks, a Survivable Group-based Public Key Management (SG-PKM) was proposed to serve as a public key infrastructure for wireless networks [37].

Above all, the selection of the key management scheme and the certificate management scheme highly depends on the intrinsic characteristics of target wireless networks, such as the network architecture, the topology dynamics, the resource constraints in terms of communication, computation and storage overheads. Moreover, these methods of the key management and the certificate management become more practical as the performance of wireless and mobile networks increase. Here, we consider that the WMN is protected by an efficient key management scheme which is beyond the scope of this paper. Furthermore, we consider that MRs take advantage of link-by-link protection, e.g., by following the IEEE 802.11 Standard [2]. This implies that all nodes support robust security network association (RSNA) and simultaneous authentication of equals (SAE). In addition, MRs adopt incremental hashing by adding (AdHASH) [38] and the elliptic curve digital signature algorithm (ECDSA) [39] in order to protect message integrity and provide tamper resistance. Furthermore, our proposed detection method is based on the following six assumptions:

1) The WMN is strongly connected, and the majority of MRs are normal. Thus, when selective forwarding attacks occur, with a high probability the transmission path can be switched to another route comprised of normal nodes.

2) The WMN is based on the IEEE 802.11 Mesh Coordination Function (MCF) contention-based Enhanced Distributed Channel Access (EDCA) protocol [2], which is extended from Distributed Coordination Function (DCF), the basic medium access control (MAC) protocol of IEEE 802.11. For simplicity, we further consider that all traffic streams have the same user priority (UP).

3) Strong security measures such as access control, authentication, encryption and inter-mesh access point controls, etc., are incorporated in the gateways so that they are resistant to attacks by adversaries. In-depth discussion on techniques addressing attacks to gateways in WMNs can be found in [40].

4) Each MR has sufficient buffer space for packet forwarding. This implies that data packets could only be dropped due to poor channel quality, medium access collisions or selective forwarding attacks.

5) Since multiple routes may exist with respect to a data flow, the source node of the flow could receive several route replies in the route discovery phase. We require the source node to buffer these routes to avoid the overhead of new route discoveries.

6) Single path transmission is used; i.e., every source node uses one transmission path at a time to transmit data packets. Multi-path transmission is out of the scope of this paper.

IV. Forwarding Assessment Based Detection Scheme

A. Overview

The proposed FADE scheme improves previous detection schemes using the two operations outlined below: 1) monitoring the behaviors of the downstream nodes based on two-hop acknowledgements and 2) multidimensional assessment based detection. We would like to emphasize that all MRs in WMNs run FADE independently. Besides, FADE is a non-cryptographic scheme and can work with different underlying routing protocols, such as AODV [31] and Optimized Link State Routing (OLSR) [41]. We also argue that the link security between two peer mesh nodes should be ensured via link-layer security protocols, e.g., as specified in [2], to defend against external attackers from overhearing, modification, forging, etc. Mesh link security protocols are used to authenticate a pair of mesh nodes and to establish session keys between them, including mesh temporal key (MTK) and mesh group temporal key (MGTK). MTK is used to protect communications between two peer mesh nodes while MGTK is used to protect group addressed MAC protocol data units (MPDUs) transmitted to peer mesh nodes. Therefore, MPDUs are protected between two peer mesh nodes. Thus the FADE scheme is designed to mitigate collusive internal attackers.

Two-hop acknowledgement based monitoring. Since we adopt mesh link security protocols to provide link-by-link encryption, conventional detection methods that rely on overhearing the wireless channel no longer work. Thus, we use the two-hop acknowledgement mechanism [26] to assess the downstream nodes behaviors. By doing this, FADE is compatible with new security features provided by the up-to-date IEEE 802.11 standard. We modify the routing tables of MRs to store the information of their two-hop neighbors.

Forwarding assessment based detection of attacks. We have shown above that collaborative grey hole attacks can evade detection of CAD, which is a typical method to detect stand-alone attackers. Hence, we propose a multidimensional assessment approach incorporating downstream and end-to-end assessments to detect potential collaborative grey hole attacks by checking for consistency between the opinion of the downstream assessment and that of the end-to-end assessment.

B. Detailed Description

To describe the FADE scheme in detail, we use the parameters and variables summarized in Table I. In addition, v_{i-1} and v_{i+1} refer to the upstream and the downstream nodes of an intermediate node v_i, respectively. The FADE scheme consists of attack information collection, attack detection and attack reaction. Under the assumption of infinite packet buffer, data packets may only be dropped due to poor channel quality, medium access collisions or selective forwarding attacks. Thus, the proposed scheme needs to differentiate real attacks from normal packet losses. We will show how to estimate the loss rate and how to select the optimal detection thresholds in Section V. In this section, we present the FADE scheme with given detection thresholds. Note that the transmission paths of multiple session flows are likely to be different from each other. Thus, the FADE scheme is designed on the basis of session flows. Here, a session can be expressed as a six-tuple $\langle snid, saddr, sport, daddr, dport, proto\rangle$, where $snid$ means the unique identification of the session flow assigned by the source node after the session is established, $proto$ refers to the transmission layer protocol in use. $saddr$/$sport$ and $daddr$/$dport$ are the source address/port and the destination address/port of the flow, respectively.

1) Attack Information Collection: In FADE, the source MR continuously sends data packets within a window at a certain

TABLE I
SUMMARY OF SYSTEM PARAMETERS AND VARIABLES

Symbol	Definition
S	Source node of a forwarding path
G	Destination gateway of a forwarding path
v_i	An intermediate node on a forwarding path
NRX_i^{i-1}	Number of data packets received by v_i from v_{i-1}
NTX_i	Number of data packets sent by node v_i
$NACK_i$	Number of two-hop acknowledgements received by v_i
WD	Window size (in terms of the number of data packets)
P_D	Distrust probability of the downstream node
P_E^i	End-to-end distrust probability of node v_i
P_{attk}	Ratio of malicious nodes in the WMN
τ_D	Downstream detection threshold
τ_E	End-to-end detection threshold
τ_D^*	Optimal downstream threshold
τ_E^*	Optimal end-to-end threshold
O_i^{i+1}	Opinion of node v_i to the downstream node v_{i+1}
O_G^i	Opinion of G to the intermediate node v_i
idn	Identification of the next hop node
$id2h$	Identification of the two-hop downstream node
idp	Identification of the previous hop node
$SIGN_i$	ECDSA signature generated by node v_i
$nonce$	Random number generated by S
k	Retransmission counter of sent CHALLENGE packets
$maxTry$	Maximum number of CHALLENGE retransmissions
$\mathbf{AR}$	Abnormal router set
C	Multiple interfaces equipped by the MRs
p_l	Estimated normal loss rate over an interface
p_b	Packet loss rate due to poor channel quality
p_m	Packet loss rate due to medium access collision
p_n	Estimated normal loss rate of a mesh link
p_a	Selective dropping rate of a malicious mesh node
R_{FP}	Total false positive rate of FADE
R_{FN}	Total false negative rate of FADE
L	Length of a transmission path

TABLE II
ALGORITHMS FOR ATTACK INFORMATION COLLECTION

Algorithm 1

Executed at the source node (S)
1. $NTX_S = 0$, $NACK_S = 0$
2. **while** $NTX_S \leq WD$ **do**
3. *SendData(G)* // send a new packet to G
4. $NTX_S = NTX_S + 1$
5. **if** *RecvAck(id2h)* **then**
6. $NACK_S = NACK_S + 1$
7. $O_S^{idn} = 0$, $P_D = NACK_S / NTX_S$
8. **if** $P_D > \tau_D$ **then**
9. $O_S^{idn} = 1$
10. *SendChallenge(S, nonce, NTX_S, O_S^{idn}, $SIGN_S$)*
11. $k = k + 1$
12. *StartTimer(reply_rx)*
13. **while** *reply_rx.expired* **and** $k \leq maxTry$ **do**
14. *SendChallenge(S, nonce, NTX_S, O_S^{idn}, $SIGN_S$)*
15. $k = k + 1$
16. *ReStartTimer(reply_rx)*
17. **if** *RecvReply(idn)* **or** $k > maxTry$ **then**
18. Activate attack reaction

Executed at an intermediate node (i)
1. $NRX_i^{idp} = 0$, $NTX_i = 0$, $NACK_i = 0$
2. **if** *RecvData(idp)* **then**
3. $NRX_i^{idp} = NRX_i^{idp} + 1$
4. *ForwardData(idn)*
5. $NTX_i = NTX_i + 1$
6. **else if** *RecvAck(id2h)* **then**
7. $NACK_i = NACK_i + 1$
8. **else if** *RecvChallenge(idp)* **then**
9. $O_i^{idn} = 0$, $P_D = NACK_i / NTX_i$
10. **if** $P_D > \tau_D$ **then**
11. $O_i^{idn} = 1$
12. **if** $idn == G$ **then**
13. *AppendToChallenge(i, NRX_i^{idp}, $SIGN_i$)*
14. **else**
15. *AppendToChallenge(i, NRX_i^{idp}, O_i^{idn}, $SIGN_i$)*
16. *ForwardChallenge(idn)*
17. **else if** *RecvReply(idn)* **then**
18. *ForwardReply(idp)*

Executed at the destination gateway (G)
1. $NRX_G^{idp} = 0$
2. **if** *RecvData(idp)* **then**
3. $NRX_G^{idp} = NRX_G^{idp} + 1$
4. *DeliverDataToUpperLayer()*
5. **else if** *RecvChallenge(idp)* **then**
6. Activate attack detection
7. **if** $\mathbf{AR} == \emptyset$ **then**
8. *SendReply(Positive)*
9. **else**
10. *SendReply(Negative, $\mathbf{AR}$)*

rate until WD packets have been sent. WD is defined as the window size in terms of the number of data packets between two consecutive CHALLENGE packets. Then, the source originates a CHALLENGE packet and sends it to the destination in order to collect attack information. Each MR maintains two packet counters in the window with respect to a session flow: one for received packets, and the other for two-hop acknowledgements. The two counters are initialized whenever the MR is selected as a relay node of the session flow. When a MR receives a new data packet from its upstream MR, it increments its received packet counter. After the MR forwards the packet to its downstream MR, it waits for the corresponding link layer acknowledgement from the downstream MR and the two-hop acknowledgement (sent in the IP-layer) from the two-hop downstream MR. The former acknowledgement is used as the evidence of its normal forwarding behaviors, and the latter one is used to prove normal forwarding behaviors of its downstream MR. Since mesh link security protocols ensure link-by-link security, we trust that acknowledgements are generated by the right MRs. When the MR receives the acknowledgement from its two-hop downstream MR, it updates the counter of two-hop acknowledgements. So, a smaller value of WD gives more timely detection of attacks but incurs more detection overheads in

a WMN. Each intermediate MR receiving the CHALLENGE packet adds its opinions towards the downstream neighbor and the number of received packets into the CHALLENGE packet. Table II shows the pseudo codes of the algorithms for attack information collection, which is run periodically in every window. Now we present an example of the CHALLENGE packet, in which we show changes of the carried message along with forwarding over a simple path. Consider a simple path consisting of four intermediate MRs, i.e., S, v_1, v_2, v_3, v_4, G. We denote the message observed by node v_i as M_i. Thus, the message carried by the CHALLENGE packet at each intermediate node is as follows:

M_1: $S \mid nonce \mid NTX_S \mid O_S^{idn} \mid SIGN_S$
M_2: $M_1 \mid v_1 \mid NRX_{v_1}^S \mid O_{v_1}^{v_2} \mid SIGN_{v_1}$
M_3: $M_2 \mid v_2 \mid NRX_{v_2}^{v_1} \mid O_{v_2}^{v_3} \mid SIGN_{v_2}$
M_4: $M_3 \mid v_3 \mid NRX_{v_3}^{v_2} \mid O_{v_3}^{v_4} \mid SIGN_{v_3}$
M_G: $M_4 \mid v_4 \mid NRX_{v_4}^{v_3} \mid SIGN_{v_4}$

The destination G uses the random number nonce to detect replay attacks. Each intermediate node protects the modified message from tampering by attaching an ECDSA signature on the digest of the message. In order to avoid attacks on the elliptic curve discrete logarithm problem, the length of private key is required to be larger than 160 bits [39]. Thus, the length of the public key (a point on the selected elliptic curve) and that of the private key are determined to be 50 bytes (400 bits) and 25 bytes (200 bits), respectively. In addition, we use AdHASH [38] to improve the efficiency of message digest generation. In AdHASH, the message to be hashed is divided into multiple blocks. The key characteristics of AdHASH are incremental hashing and fast modulo addition. As an example, we denote $M = m_1 \cdots m_p$ and $M' = Mm_{p+1} \cdots m_{p+q}$ as the original message and the modified message, respectively, and m_i $(i = 1, \ldots, p)$ as the ith block of M. Then, the final hash value of M' is $hash(M') = hash(Mm_{p+1} \cdots m_{p+q}) = hash(M) + hash(m_{p+1} \cdots m_{p+q}) = hash(M) + hash(m_{p+1}) + \cdots + hash(m_{p+q})$. Hence, it only needs additional q hashing and q modulo addition operations to generate the hash value for M'. In a practical design, we select $hash$ to be SHA-1 [42].

2) Attack Detection: When the destination receives the CHALLENGE packet, it retrieves attack information regarding all intermediate MRs. Furthermore, the destination gives an opinion about each intermediate node by examining its end-to-end distrust probability. Then, the opinion of the destination is compared with that of the upstream neighbor. The pseudo code of the algorithms for attack detection is shown in Table III. Taking some intermediate node vi as an example, there are four possible cases:

1) $O_{i-1}^i = 0$ and $O_G^i = 0$. This case means that no selective forwarding attack exists, and node v_i is behaving normally.

2) $O_{i-1}^i = 1$ and $O_G^i = 1$. This case indicates a stand-alone grey hole attack by node v_i. Node v_{i-1} accuses its downstream node v_i by obtaining the distrust probability of v_i larger than the threshold τ_D. Meanwhile, the number of packets received by v_{i+1} from v_i is less than $WD \cdot (1-\tau_E)$, resulting in the end-to-end distrust probability of v_i to be larger than the threshold τ_E. Therefore, both O_{i-1}^i and O_G^i are set to 1.

3) $O_{i-1}^i = 0$ and $O_G^i = 1$. This case indicates a collaborative grey hole attack by malicious nodes v_{i-1} and v_i. In this case, no matter what the results of downstream distrust probability are, node v_{i-1} refrains from accusing its partner v_i, which results in $O_{i-1}^i = 0$. However, the normal node v_{i+1} marks the number of received packets from v_i into the CHALLENGE message honestly. Then, the gateway G will detect these collusive nodes by obtaining the end-to-end distrust probability of v_i larger than the threshold τ_E. Hence, $O_G^i = 1$.

4) $O_{i-1}^i = 1$ and $O_G^i = 0$. This case suggests two possible attacks. One is the malicious accusation attack by node v_{i-1}, and the other is the counterfeit mark attack by node v_{i+1}. For the former attack, node v_{i-1} intentionally accuses its downstream node v_i regardless of its normal forwarding behaviors. Hence, $O_{i-1}^i = 1$. However, the value of NRX_{i+1}^i marked by node v_{i+1} gives a positive evidence that node v_i has forwarded all packets. Therefore, $O_G^i = 0$. Regarding the latter attack, node v_i, in fact, drops a portion of the packets. Node v_{i-1} accuses its downstream node by obtaining the distrust probability of v_i larger than the threshold τ_D. So, $O_{i-1}^i = 1$. However, the malicious node v_{i+1} tampers the number of packets received from v_i to satisfy $NRX_{i+1}^i < WD \cdot (1-\tau_E)$. Hence, $O_G^i = 0$. A feasible method to distinguish the two attacks is to check the link acknowledgements received by v_i from v_{i+1}. If node v_i generates enough positive evidences to indicate that it is forwarding packets honestly, then the former attack occurs, otherwise the latter one happens.

3) Attack Reaction: As shown in Table II, after the gateway G receives a CHALLENGE message from the source node S, G sends a REPLY message indicating potential malicious MRs. In order to protect the REPLY message from tampering, an ECDSA signature signed by G is attached. Moreover, the random number nonce extracted from the CHALLENGE

TABLE III
ALGORITHMS FOR ATTACK DETECTION

Algorithm 2

1. $\mathbf{AR} = \emptyset$
2. **for** $id = G$ **to** the next hop of S **do**
3. Denote uid as the ID of id's upstream node
4. *VerifySignature*($SIGN_{uid}$)
5. **if** verification fails **then**
6. $\mathbf{AR} = \mathbf{AR} \cup \{uid\}$
7. $O_G^{uid} = 0$, $P_E^{uid} = 1 - NRX_{id}^{uid}/WD$
8. **if** $P_E^{uid} > \tau_E$ **then**
9. $O_G^{uid} = 1$
10. **for** $id = S$ **to** idp **do**
11. Denote did as the ID of id's downstream node
12. Denote $d2hid$ as the ID of did's downstream node
13. **if** $O_{id}^{did} == 0$ **and** $O_G^{did} == 1$ **then**
14. $\mathbf{AR} = \mathbf{AR} \cup \{id, did\}$
15. **else if** $O_{id}^{did} == 1$ **and** $O_G^{did} == 0$ **then**
16. $\mathbf{AR} = \mathbf{AR} \cup \{id, d2hid\}$
17. **else if** $O_{id}^{did} == 1$ **and** $O_G^{did} == 1$ **then**
18. $\mathbf{AR} = \mathbf{AR} \cup \{did\}$
17. **else**
18. $\mathbf{AR} = \mathbf{AR} \cup \emptyset$
19. **return** $\mathbf{AR}$

message is inserted into the REPLY message to defeat the replay attack. The source node S performs attack reaction after receiving the REPLY message or the value of k exceeds $maxTry$. Therefore, there are three cases listed as follows:

1) S receives a Positive REPLY. This case indicates that all intermediate nodes along the path are behaving normally. Therefore, S continues transmitting data packets in the next window.

2) S receives a Negative REPLY. This case implies that there are some attacks in the routing path. From the REPLY message, S obtains a list of suspicious nodes, i.e., $\mathbf{AR}$. Then, the source can filter falsely accused nodes using an evidence collection mechanism, which is out of our current design. Once the list of malicious nodes is determined, the source switches the transmission path to the one that does not involve any node in the list.

3) The value of k exceeds $maxTry$. This case appears due to three possible reasons: a) The CHALLENGE packet is dropped by some malicious node; b) The REPLY packet is dropped by some malicious node; c) Poor channel quality or medium access collisions. In [9], the authors proposed a hop-by-hop query method to locate the malicious nodes. However, the method requires the source node to send a few query packets, which incurs a lot of overheads. Hence in FADE, we select another path in the route buffer to provide a route for subsequent packets. The motivation of our method is to mitigate the overheads of hop-by-hop query. Although identification of the malicious nodes (if they truly exist) may be delayed, the routing security is ensured by using a new route under the assumption that the majority of MRs are normal.

C. Discussion

We investigate some details of the proposed scheme and discuss its cost and other issues in practical usage.

1) Forged Two-hop Acknowledgement: As mentioned before, the two-hop acknowledgement is implemented at the network layer. So, it is possible for a two-hop downstream attacker to modify the acknowledgement, resulting in a false negative opinion on the downstream node (if it is actually normal). However, we can identify this case by integrating the corresponding end-to-end opinion with link layer evidences possessed by the victim node. As long as the source node collects enough evidences from the victim and gets a positive end-to-end opinion, the falsely accused victim will be removed from $\mathbf{AR}$. Hence, secure evidence collection is of great concern. Since MRs in infrastructure WMNs are mostly deployed in a stationary manner, it is feasible to use a pre-allocated side channel that is unknown to other nodes, to securely transmit evidences from the victim to the source. A drawback is that allocating side channels increases the system cost somewhat.

2) Computation and Memory Overheads Reduction: Since we exploit several cryptographic techniques to defend against outside attackers, computation and memory overheads are of great concern in real networks. Due to various constraints, it is not possible to give a thorough evaluation of computation and memory consumption in this paper. Here, we briefly discuss methods for overhead reduction. In FADE, the length of the public key and that of the private key are determined to be 50 bytes (400 bits) and 25 bytes (200 bits), respectively, to meet the security requirements of ECDSA [39]. Thus, each MR stores 75 bytes of keys for itself, while the gateway stores not only its own keys but also all public keys of the MRs in the WMN. Hence, the storage cost of the gateway with respect to ECDSA keys is $(75 + 50N)$ bytes, where N is the number of MRs in the network. There are two possible ways to reduce the memory overhead: 1) Using shorter keys for security assurance; 2) Delegating signature verification to a trusted third party. Then, the gateway does not need to store public keys of all MRs. As a matter of fact, it is also an effective way to reduce computation overheads of generating and updating FADE messages. However, the latter method incurs higher bandwidth consumption and detection delay. In general, there is a tradeoff between cost and performance in security mechanism design.

3) Performance Improvement of FADE: As described above, the sensitive information of all the nodes that comprise a route is correlated by the destination node to detect attackers. Thus, the delay of attack detection highly depends on the route length. To reduce this delay, we propose to divide the whole WMN into multiple domains. Assume that each domain has a powerful MR, which hosts a security authority (SA) agent that is capable of performing attack detection and reaction. To speed up the assessment of grey hole attacks, the node on the border of a domain sends currently collected information to the SA. Then, the SA performs domain assessment (a variant of the combination of downstream assessment and end-to-end assessment), and then replies to the source node. Although the method can improve the performance of FADE, the security of MRs running SA must be assured, or else this performance improvement method may compromise the security of the WMN.

V. Determination of Detection Thresholds

Note that in ad hoc routing it is usually assumed that there are some criteria to determine whether a node is a neighbor or not, depending on the quality of the link to this node. A poor link quality would cause breakage of the established route and trigger a route maintenance. Since this paper is concerned with grey hole attack at the network layer, route breakages and maintenance are not taken into consideration here. Furthermore, adjacent MRs can relay packets using different non-overlapping channels to mitigate intra-flow interferences, thus normal packet losses are assumed to be independent events at different MRs. Based on these assumptions, we present the results of τ_D^* and τ_E^* by minimizing the sum of the false positive and false negative rates of FADE.

A. Normal Loss Rate

The normal packet loss rate p_l over an interface c is calculated by

$$p_l(c) = p_b + p_m - p_b \cdot p_m, \tag{1}$$

where p_b and p_m, respectively, denote the packet loss rates due to poor channel quality and medium access collisions.

Furthermore, we focus on packet losses due to the selective forwarding attack and consider that the normal packet loss rate is much smaller than the selective dropping rate when a forwarding attack is ongoing. Then, the estimated normal loss rate of a mesh link is approximately defined as the maximum normal loss rate over all interfaces, i.e.,

$$p_n = \max_{c \in C} p_l(c). \tag{2}$$

Similar to [9], we model the underlying wireless channel as the two-state Markov model, also known as the Gilbert model, regarding the packet loss due to poor channel quality. The model has two states known as the good state and bad state. Let p_{gb} denote the transition probability from the good state to the bad one, and p_{bg} vice versa. The meaning of p_{gb} (or p_{bg}) is the probability that the next packet is lost (or delivered), provided the previous one has been delivered (or lost). Note that usually $p_{gb} < p_{bg}$. Then, the steady state probabilities denoted respectively by π_g and π_b for the good and bad states can be computed as $\pi_g = p_{bg}/(p_{bg}+p_{gb})$ and $\pi_b = p_{gb}/(p_{bg}+p_{gb})$. To calculate p_{bg} and p_{gb}, a feasible way is using the loss length distribution statistics, which has been discussed in detail in [43]. Hence, we define the normal loss rate due to poor channel quality by

$$p_b = \pi_b = p_{gb}/(p_{bg} + p_{gb}). \tag{3}$$

Regarding packet losses due to medium access collisions, we consider that the WMN employs IEEE 802.11 MCF EDCA. For simplicity, we also assume that all traffic streams have the same UP, in which case MCF reduces to the same access method as DCF [2]. We adopt the analytical results in [9] to estimate the packet loss rate due to medium access collisions. Therefore, the relationships among channel busy ratio (R_b), the probability that a node transmits in a time slot (p_t) and the normal loss rate due to medium access collisions (p_m) are given by

$$\begin{cases} p_i = (1-p_t)^n \\ p_s = n \cdot p_t \cdot (1-p_t)^{n-1} \\ p_c = 1 - p_i - p_s \end{cases} \tag{4}$$

$$R_b = 1 - (p_i \cdot \sigma)/(p_i \cdot \sigma + p_s \cdot T_s + p_c \cdot T_c), \tag{5}$$

$$p_m = 1 - (1-p_t)^{n-1}, \tag{6}$$

where p_i, p_s and p_c are the steady state probabilities of idle, successful and colliding slots, respectively [9]; n is the number of nodes contending for channel access; σ, T_s and T_c are the slot length, the duration of a successful transmission and the duration of a collision, respectively, as derived from [2].

B. The Optimal Detection Thresholds

Since FADE detects selective forwarding attacks based on downstream and end-to-end assessments using the above thresholds, the false positive and false negative rates of FADE highly depend on these thresholds. Larger thresholds give a lower false positive rate but a higher false negative rate. We further consider that the false positive and false negative rates have the same weight because a good detection scheme should consider both false positives and false negatives in order to gain considerable performance.

1) The Total False Positive Rate: When normal losses exist, a false alarm occurs when a packet drop due to normal loss is falsely attributed to selective forwarding attack. In fact, FADE detects selective forwarding attacks by comparing the monitored loss rate with the detection thresholds. Then, a burst of normal losses may cause a false alarm if the ratio of packet losses to the number of transmitted packets in a window exceeds the downstream or the end-to-end threshold. On the other hand, since FADE is based on multidimensional assessments, we need to analyze the total false positive rate over a transmission path.

Downstream false positive rate. Each intermediate node v_i gives its opinion on the behaviors of the downstream node by calculating the ratio of the number of two-hop acknowledgements received from v_{i+2} to the number of sent packets. Let N_{pkt} denote the number of data packets sent by v_i in a window. Thus, the number of packet losses without triggering a FADE alarm is no more than $N_{pkt} \cdot \tau_D$. When there is no attack in the WMN, a downstream false alarm appears if and only if the number of normal losses exceeds $N_{pkt} \cdot \tau_D$. Therefore, the downstream false positive rate, denoted as R^v_{FP}, is given by

$$\begin{aligned} R^v_{FP} &= \sum_{i=N_{pkt}\cdot\tau_D+1}^{N_{pkt}} \binom{N_{pkt}}{i} \cdot p_n^i \cdot (1-p_n)^{N_{pkt}-i} \\ &= 1 - \sum_{i=0}^{N_{pkt}\cdot\tau_D} \binom{N_{pkt}}{i} \cdot p_n^i \cdot (1-p_n)^{N_{pkt}-i}. \end{aligned} \tag{7}$$

When N_{pkt} is sufficiently large, a reasonable approximation to the binomial distribution $B(N_{pkt}, p_n)$ is given by the normal distribution with mean $N_{pkt} \cdot p_n$ and variance $N_{pkt} \cdot p_n \cdot (1-p_n)$, i.e., $N(N_{pkt} \cdot p_n, (N_{pkt} \cdot p_n \cdot (1-p_n))^{1/2})$ [44]. Furthermore, we apply a continuity correction of 0.5 to improve the accuracy of the Normal approximation to binomial probabilities. Thus, the definition of R^v_{FP} in (7) can be reformed to

$$R^v_{FP} \approx 1 - \frac{1}{\sqrt{2\pi}} \int_{\frac{-N_{pkt}\cdot p_n - 1/2}{\sqrt{N_{pkt}\cdot p_n \cdot (1-p_n)}}}^{\frac{N_{pkt}\cdot\tau_D - N_{pkt}\cdot p_n + 1/2}{\sqrt{N_{pkt}\cdot p_n \cdot (1-p_n)}}} e^{-\frac{1}{2}x^2} dx. \tag{8}$$

End-to-end false positive rate. The gateway gives its opinion on whether a suspicious node exists or not by comparing the number of data packets received by some intermediate node from its upstream node within the window. Let d denote the maximum difference between the length of the window and the number of received packets with respect to each intermediate node on a given path. When there is no attack in the WMN, an end-to-end false alarm appears if and only if $d > WD \cdot \tau_E$. Hence, the end-to-end false positive rate, denoted as R^e_{FP}, is given by

$$\begin{aligned} R^e_{FP} &= \sum_{d=WD\cdot\tau_E+1}^{WD} \binom{WD}{d} \cdot p_n^d \cdot (1-p_n)^{WD-d} \\ &\approx 1 - \frac{1}{\sqrt{2\pi}} \int_{\frac{-WD\cdot p_n - 1/2}{\sqrt{WD\cdot p_n \cdot (1-p_n)}}}^{\frac{WD\cdot\tau_E - WD\cdot p_n + 1/2}{\sqrt{WD\cdot p_n \cdot (1-p_n)}}} e^{-\frac{1}{2}x^2} dx. \end{aligned} \tag{9}$$

Total false positive rate. As we discussed before, FADE alerts an anomaly if any of the following three cases occurs:

(a) an alarm triggered by downstream assessments; (b) an alarm triggered by end-to-end assessments; (c) both (a) and (b). Therefore, the total false positive rate of FADE is

$$\begin{aligned} R_{FP} &= 1-(1-R_{FP}^{v})^{L}+R_{FP}^{e}-[1-(1-R_{FP}^{v})^{L}]\cdot R_{FP}^{e} \\ &= 1-(1-R_{FP}^{e})\cdot(1-R_{FP}^{v})^{L}. \end{aligned} \tag{10}$$

2) The Total False Negative Rate: A missed detection event occurs if FADE does not raise an alarm when selective forwarding attacks exist.

Downstream false negative rate. No downstream alarm occurs if the number of packet losses is no more than $N_{pkt}\cdot\tau_D$. Therefore, the downstream false negative rate, denoted as R_{FN}^{v}, is given by

$$\begin{aligned} R_{FN}^{v} &= \sum_{i=0}^{N_{pkt}\cdot\tau_D}\binom{N_{pkt}}{i}\cdot(p_n+p_a)^{i}\cdot(1-p_n-p_a)^{N_{pkt}-i} \\ &\approx \frac{1}{\sqrt{2\pi}}\int_{\frac{-N_{pkt}\cdot(p_n+p_a)-1/2}{\sqrt{N_{pkt}\cdot(p_n+p_a)\cdot(1-p_n-p_a)}}}^{\frac{N_{pkt}\cdot\tau_D-N_{pkt}\cdot(p_n+p_a)+1/2}{\sqrt{N_{pkt}\cdot(p_n+p_a)\cdot(1-p_n-p_a)}}} e^{-\frac{1}{2}x^{2}}dx. \end{aligned} \tag{11}$$

End-to-end false negative rate. No end-to-end alarm occurs if the number of packet losses is no more than $WD\cdot\tau_E$. Hence, the end-to-end false negative rate, denoted as R_{FN}^{e}, is given by

$$\begin{aligned} R_{FP}^{e} &= \sum_{d=0}^{WD\cdot\tau_E}\binom{WD}{d}\cdot(p_n+p_a)^{d}\cdot(1-p_n-p_a)^{WD-d} \\ &\approx \frac{1}{\sqrt{2\pi}}\int_{\frac{-WD\cdot(p_n+p_a)-1/2}{\sqrt{WD\cdot(p_n+p_a)\cdot(1-p_n-p_a)}}}^{\frac{WD\cdot\tau_E-WD\cdot(p_n+p_a)+1/2}{\sqrt{WD\cdot(p_n+p_a)\cdot(1-p_n-p_a)}}} e^{-\frac{1}{2}x^{2}}dx. \end{aligned} \tag{12}$$

Total false negative rate. FADE fails to give an alarm if both downstream assessments and end-to-end assessments fail not detect packet loss events caused by selective forwarding attacks. Thus, the total false negative rate of FADE is

$$R_{FN} = (R_{FN}^{v})^{L}\cdot R_{FN}^{e}. \tag{13}$$

3) Computation of the Optimal Thresholds: Based on (10) and (13), we find that the total false positive rate increases as each threshold increases but the total false negative rate decreases. Since the sum of R_{FP} and R_{FN} is a convex function with respect to τ_D and τ_E, we can derive the optimal thresholds (τ_D^{*} and τ_E^{*}) according to

$$\frac{d}{d\tau_D}(R_{FP}+R_{FN})\mid_{\tau_D=\tau_D^{*}}=0 \tag{14}$$

$$\frac{d}{d\tau_E}(R_{FP}+R_{FN})\mid_{\tau_E=\tau_E^{*}}=0. \tag{15}$$

As shown in (9) and (12), we use the Normal distribution as an approximation to the Binomial distribution when the window size is large enough. As a rule of thumb [44], values of WD and p satisfy $WD\cdot p\geq 10$ and $WD\cdot(1-p)\geq 10$, where $p=p_n$ for (9) and $p=p_n+p_a$ for (12). Therefore, we can compute the optimal thresholds by applying the Chain rule and the Leibniz's rule [45] according to (14) and (15).

VI. Performance Evaluations

A. Simulation Setup

We use network simulator ns2 (v2.33) for simulations and evaluate the performance of FADE in terms of Packet Delivery Ratio (PDR) and Overhead per Data Bit (ODB). As we mentioned before, under the assumption that all traffic streams have the same UP, the IEEE 802.11 MCF EDCA protocol employed by MRs in the WMN has the same performance as DCF, which is the default MAC protocol in the ns2 library. Thus, we used this MAC protocol for all the simulations. Furthermore, we separately implemented FADE based on the AODV protocol [31], a classical on-demand routing protocol, and the OLSR protocol [41], a typical link state routing protocol. Unless explicitly specified with the results, AODV is the underlying routing protocol used in the corresponding experiments. All MRs in the WMN independently run FADE to detect selective forwarding attacks.

The evaluated network in the simulations consists of a square grid of 36 evenly-spaced stationary nodes (numbered from node 0 to node 35 column by column) located in a 750m750m square. Node 0 at one corner serves as the source node of the default data flow, while node 7 is the source of the second data flow. Both data flows start at simulation time of 5s and their destinations are set to node 35 (at the opposite corner to node 0), which functions as the gateway. The source nodes originate User Datagram Protocol (UDP) / constant bit rate (CBR) flows with a packet size of 200 bytes to its intended gateway. The average number of malicious nodes, which are randomly selected via a random number generator, is determined with the parameter P_{attk}. For simplicity, malicious nodes have the same selective dropping rate and perform grey hole attacks when simulations start. Moreover, stand-alone attackers honestly assess each other, similar to what normal nodes behave in downstream assessments, while collusive attackers refrain from accusing each other if they are neighbors of each other. We also assume that all the interfaces have the same wireless channel model. Each simulation lasts 300 seconds, and each data point in the simulation results is an average of 20 independent runs. More parameters are listed as follows: Transmission range and vertical/horizontal distances between adjacent nodes are set to 250 meters and 150 meters, respectively. Omni-antenna is used as the antenna model, and the Gilbert model is adopted to model the underlying wireless channel. Furthermore, since there are three non-overlapping channels for IEEE 802.11b/g [2] in the 2.4GHz Industrial, Scientific and Medical band, and the basic 802.11 DCF MAC layer protocol is implemented in the ns2 simulator by default, the number of interfaces per node is set to 3 in our experiments in order to reduce interferences between successive hops. Note that the proposed scheme is also effective when the number of non-overlapping channels increases by letting the MAC layer protocol work according to another specification in the set of IEEE 802.11 standards, such as the IEEE 802.11a working in 5.8GHz. One reason is that the routing protocol utilizes multiple channels to reduce interferences, and the other reason is that the proposed scheme intends to detect grey hole attacks that occur in the network layer. Thus, the selection of the

MAC layer protocol does not have great influence on the performance of the proposed scheme. Moreover, the parameter $maxTry$ is assigned the same value of 2 as in [9] for the convenience of comparison.

We evaluate the performance of FADE in four cases. Firstly, we examine the adjustment of the optimal detection thresholds regarding the network load. We change the number of data flows and the data bit rate to illustrate the adaptation of FADE to network dynamics. Taking the default data flow originated from node 0 that is at the opposite corner of the grid to the gateway, we then evaluate the performance of FADE with respect to different window sizes. Since a larger window results in a higher loss rate under attacks as well as a smaller overhead, we would like to select a proper window length to tradeoff the two contradictory metrics. Furthermore, we investigate the performance of FADE with different ratios of malicious nodes to test its effectiveness under varied threat levels and different underlying routing protocols. Lastly, we compare the proposed scheme with CAD [9] and Sprout [28] regarding different ratios of malicious nodes under stand-alone and collaborative grey hole attacks.

B. Simulation Results and Analysis

Before we present the simulation results, we define effective bytes in a packet as the payload length of the packet expressed in terms of bytes. Furthermore, we define PDR and ODB as follows: the PDR of a flow is the number of data packets received by the gateway divided by the number of data packets sent by the source, and the ODB is defined by

$$ODB = (L_{RT} + L_{FADE})/L_{DATA}, \tag{16}$$

where L_{RT} and L_{FADE} are the total number of effective bytes in routing messages and FADE packets (including CHALLENGE and REPLY), which are sent or forwarded by MRs, respectively. L_{DATA} is the total number of effective bytes in data packets received by the gateway. Specifically, we examine the changes of ODB regarding different values of WD to evaluate the overhead of the proposed scheme when the WMN is in the steady state. Then, we validate our analytical results through simulations. Let L_D be the length of a data packet, and L_C and L_R refer to the lengths of the CHALLENGE and REPLY packets, respectively. We further denote L_F as $L_C + L_R$. Since grey hole attacks or normal packet losses result in dropping data packets, the total number of effective bytes of data packets received in each window is

$$L_{DATA} = L_D \cdot WD \cdot (1-p_n)^l \cdot (1-p_a)^{P_{attk} \cdot l}, \tag{17}$$

where l is the route length. On the other hand, the source node would retransmit the CHALLENGE message if it fails to receive REPLY message within a certain time. Therefore, average number of effective bytes of FADE packets between two continuously retransmitted CHALLENGE messages is approximately $((l-1)/2) \cdot L_F$. Thus, the total number of effective bytes of FADE packets is given by

$$L_{FADE} \leq \sum_{k=1}^{maxTry} \left[\frac{(k+1)(l-1)}{2} p_d^2 L_F (1-p_d^2)^{k-1} \right], \tag{18}$$

where $p_d = (1-p_n)^l$ is the probability of a successful transmission.

Then, when the WMN is in the steady state, the overhead of FADE in terms of ODB is given by

$$ODB^* = L_{FADE}/L_{DATA}. \tag{19}$$

Finally, we have

$$ODB^* \leq \frac{(l-1)L_F \left[1 + p_d^2 - (1 + p_d^2 + K p_d^2)(1-p_d^2)^K \right]}{2 \cdot WD \cdot L_D \cdot p_d^3 \cdot (1-p_a)^{P_{attk} \cdot l}}, \tag{20}$$

where K is an alias name of $maxTry$.

1) Adjustment of the Optimal Thresholds With Respect to the Network Load: In this part, we evaluate the ability of FADE to adapt to network dynamics, where WD and p_a are set to 200 and 10%, respectively. Fig. 2 illustrates the adaptation of the optimal downstream threshold with respect to varied network load in terms of the number of data flows and the data bit rate. We have two main observations from Fig. 2. Firstly, τ_D^* increases with a larger data bit rate when the number of data flows is fixed. Secondly, τ_D^* also increases if the number of data flows increases. In the former case, a larger

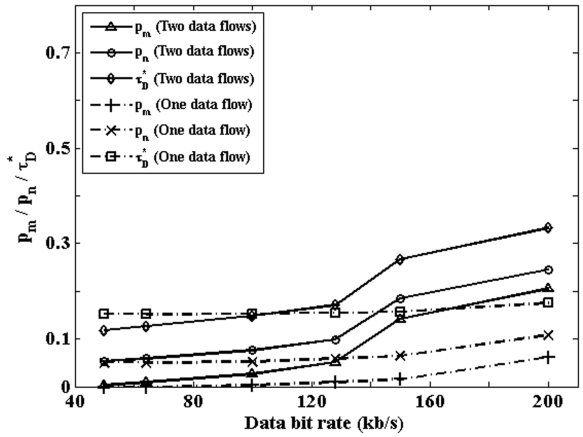


Fig. 2. The optimal downstream threshold versus the network load, where $p_a = 10\%$, $p_{gb} = 0.052$ and $p_{bg} = 0.99$.

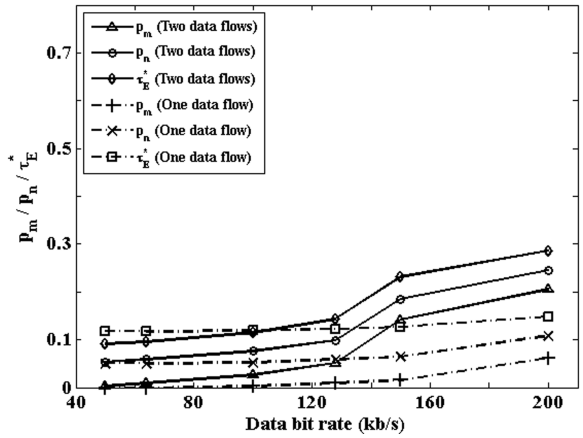


Fig. 3. The optimal end-to-end threshold versus the network load, where $p_a = 10\%$, $p_{gb} = 0.052$ and $p_{bg} = 0.99$.

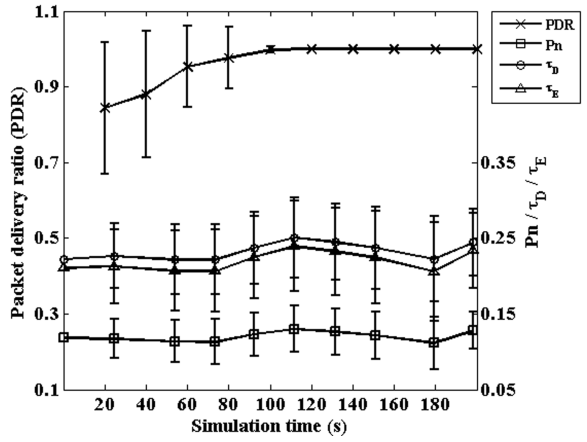


Fig. 4. Results of adjusting thresholds with random normal loss rates and statistical results of PDR, where FADE = ON, $P_{attk} = 0.3$ and $p_a = 30\%$.

bit rate incurs a bigger probability of medium access collision (see the change of p_m). Then, the estimated normal loss rate p_n increases as well according to (1) and (2), as depicted in Fig. 2. To avoid a high false positive rate, the optimal threshold τ_D^* adapts accordingly. Similarly in the latter case, the estimated normal loss rate might increase due to traffic interferences. Thus, the optimal threshold τ_D^*, compared with the case of one data flow, also increases if two data flows coexist in the simulated network. From Fig. 3, we can make similar conclusions on the adaptation of the optimal end-to-end threshold. When the data bit rate or the number of data flows raises, the optimal threshold τ_E^* increases with the normal loss rate p_n. From Fig. 2 and Fig. 3, we see that FADE can adapt to network dynamics due to varied network load.

To further evaluate the adaptation of FADE in real time, we carried out another group of simulations in which the channel quality varied with time. We set the ratio of the number of collusive attackers to the network size (P_{attk}) to 0.3. We also selected a value of selective dropping rate (p_a) as 0.3 and activated the FADE scheme. In each simulation, we randomized the parameters of the Gilbert model to generate varied channel quality. Typically, the value of p_b was randomly selected from 0.05 to 0.15. Fig. 4 illustrates results of adjusting thresholds with random normal loss rates and statistical results of PDR. On one hand, we observe that both τ_D and τ_E keep pace with p_n, and the values of p_n, τ_D and τ_E do not dramatically fluctuate in different simulation runs. On the other hand, the PDR curve shows that FADE effectively maintains the overall performance of data transmissions. Moreover, the figure shows that PDR stabilizes with time. These results highlight the fact that FADE can adapt to changes of normal loss rates.

2) Performance of FADE Versus Window Size: Fig. 5 and Fig. 6 illustrate the performance of FADE in terms of PDR and ODB with respect to WD and p_a, respectively, where $P_{attk} = 0.18$. We see in Fig. 5 that PDR decreases with an increase of WD. It is obvious that a big window reduces the frequency of transmitting CHALLENGE packets. So, it suffers delays to detect malicious nodes in the network. Fig. 5 also shows that PDR decreases when the selective dropping rate increases. On the other hand, Fig. 6 depicts that both analytical and experimental results of ODB dramatically decrease with an increase of WD. In addition to the same reason as above, i.e., a low frequency of transmitting CHALLENGE packets reduces the total number of FADE packets, another reason for this observation is the large size of a FADE packet compared to that of a data packet. Since all intermediate nodes use ECDSA to protect messages, they attach a new signature to each received FADE packet before forwarding it to their next hop. Moreover in Fig. 6, the experimental results of ODB with $p_b = 0.1$ are consistent with the analytical results, which lends confidence to the correctness of (20). According to the above results, we empirically limit the value of WD to [1000, 1400], which is a good tradeoff between the PDR (greater than 0.9) and the ODB (less than 0.18). Therefore, we set WD to 1000 in the following.

3) Impact of FADE on Network Performance: We examine two cases for each underlying routing protocol, i.e., with the FADE scheme (denoted as "FADE = ON") and without the FADE scheme (denoted as "FADE = OFF"), where $WD = 1000$ and $p_a = 30\%$. Fig. 7 illustrates the results of adjusting the number of attackers with different states of FADE. We

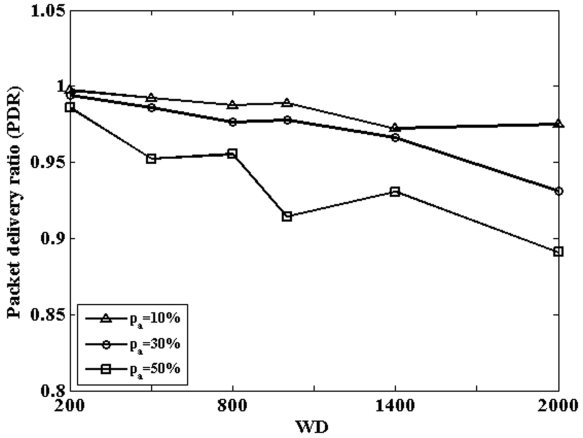


Fig. 5. Performance of FADE in terms of PDR versus window size WD with different values of p_a, where $P_{attk} = 0.18$.

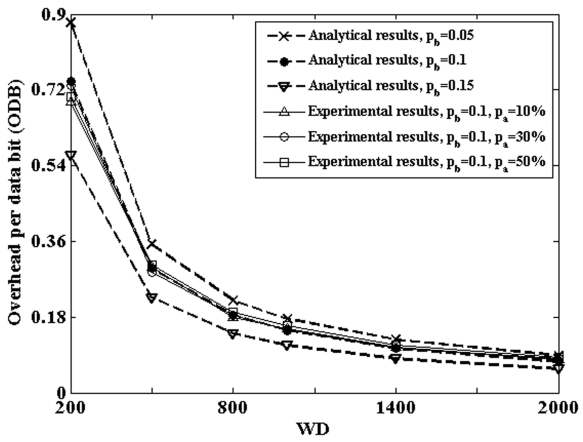


Fig. 6. Performance of FADE in terms of ODB versus window size WD with different values of p_a, where $P_{attk} = 0.18$.

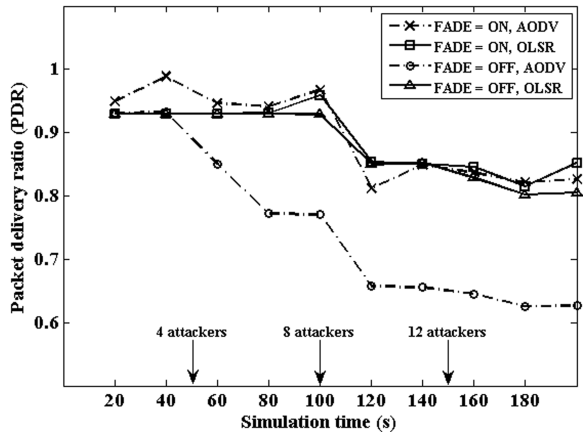


Fig. 7. Results of adjusting the number of attackers with different states of FADE and statistical results of PDR, where $WD = 1000$ and $p_a = 30\%$.

see that the PDR dramatically decreases with the increase of the number of attackers when FADE = OFF. However, the PDR performance maintains a high level when FADE = ON. We also observe in Fig. 7 that no matter what the routing protocol is, the PDR in the case of FADE = ON outperforms the FADE = OFF case. The results justify that FADE can be applied to different routing protocols. Taking the AODV version FADE as an example, we see that the PDR is less than 0.65 when FADE = OFF and the number of attackers is 12. On the contrary, when FADE = ON, the proposed scheme enhances the PDR to about 0.83. Since stand-alone malicious nodes appear with a high probability when the number of attackers is small and collusive ones appear as the number of attackers increases, the results highlight that FADE is effective to defeat different types of grey hole attacks.

4) Performance Comparisons with Other Schemes: In this part, we compare the FADE scheme with CAD and Sprout. To evaluate these schemes, channel overhearing is considered to be valid for use in CAD. Similarly, we set WD and p_a to 1000 and 30%, respectively.

FADE vs CAD. Fig. 8 shows that both FADE and CAD can protect the network against stand-alone grey hole attacks. The reason is that whenever a malicious node drops a certain number of data packets, its upstream node on the forwarding path gives a negative opinion on the node. Then, the source node will receive a negative reply and select a new route to transmit subsequent data. However, in the case of collaborative grey hole attacks, we see in Fig. 8 that the PDR of CAD decreases significantly. As we described before, the node that drops data packets will falsely mark the number of packets received from its upstream partner. Then, the downstream normal node always fails to give negative upstream opinions on the attacker. On the other hand, the upstream partner of the attacker will not give negative opinions of the attacker. Therefore, CAD is unable to detect such sophisticated attacks. FADE, on the contrary, is able to defeat collusive attackers by using the end-to-end assessment based on the fact that all downstream normal nodes honestly mark the number of data packets received in a window. Thus, FADE can detect such attacks when at least one normal node locates at the downstream part of paths. Therefore, the PDR of FADE is higher than CAD under collaborative attacks.

FADE vs Sprout. Since Sprout is a source-routed, link-state, multi-path routing protocol [28], we compare the proposed scheme with Sprout using the OLSR version of FADE in this part. Fig. 9 illustrates that no matter how multiple malicious nodes behave, the PDR of FADE under collusive attackers has no apparent differences from that under stand-alone attackers. We also observe similar results for Sprout. Thus, both FADE and Sprout are effective to defeat collusive attackers. Furthermore, we see that the PDR of FADE is higher than Sprout. As indicated in [28], Sprout adopts probabilistic route generation and stochastic path selection with route performance feedback to maintain the overall performance of networks. However, it is possible to use some existing routes that have been polluted by malicious nodes to transmit data packets. FADE, on the contrary, ignores those polluted paths in packet forwarding. Specifically, the OLSR version of FADE checks the node list of a candidate path. If one or more malicious nodes exist, then the candidate is

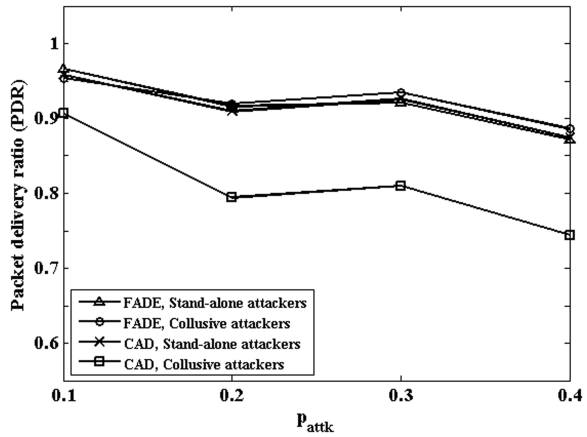


Fig. 8. Comparison of FADE and CAD using on-demand routing protocols: PDR versus ratio of malicious nodes P_{attk} under stand-alone and collaborative grey hole attacks, where $WD = 1000$ and $p_a = 30\%$.

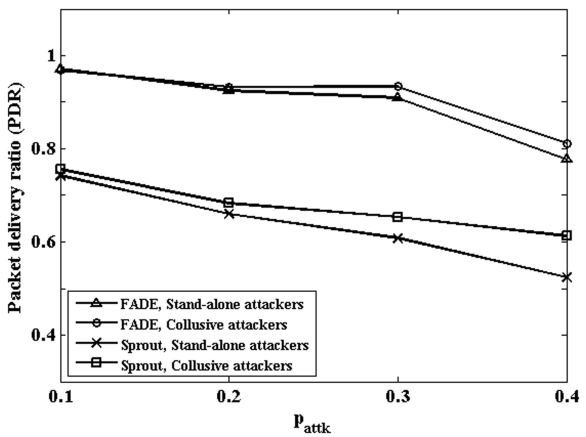


Fig. 9. Comparison of FADE and Sprout using link-state routing protocols: PDR versus ratio of malicious nodes P_{attk} under stand-alone and collaborative grey hole attacks, where $WD = 1000$ and $p_a = 30\%$.

ignored. FADE is able to accomplish this because valid routes are established prior to data transmission when OLSR is the underlying routing protocol. Whenever some clean routes are valid for use between the source and the gateway, FADE can gain better performance than Sprout.

The experimental results presented highlight the fact that compared with other schemes, FADE is more capable of detecting sophisticated attacks. Furthermore, FADE is able to adapt to network dynamics, such as poor channel quality and medium access collisions.

VII. Conclusion

In this paper, we have proposed a forwarding assessment based detection scheme, which combines downstream assessments and end-to-end assessments to detect sophisticated selective forwarding attacks. In particular, MRs monitor forwarding behaviors of their downstream nodes via two-hop acknowledgements. By using the monitoring method instead of the classical channel overhearing, the proposed scheme is compatible with security features at the link layer such as those provided by the up-to-date IEEE 802.11 standard. To maximize the detection accuracy, we have carried out theoretical analysis on the optimal detection thresholds under normal losses due to poor channel quality or medium access collisions. Our results demonstrate that the proposed scheme, compared with existing detection schemes, is effective against both stand-alone and collaborative grey hole attacks while incurring a small overhead. Note that this work addresses detection but not countermeasures against colluding malicious MRs, which is an interesting area for further studies.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Comput. Networks*, vol. 47, no. 4, pp. 445–487, 2005.

[2] *IEEE Standard for Information Technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, IEEE Std. 802.11-2012 (Revision of IEEE Std 802.11-2007), 2012.

[3] H.-M. Sun, C.-M. Chen, and Y.-C. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in *TENCON'07*, 2007, pp. 1–4.

[4] M. Tiwari, K. V. Arya, R. Choudhari, and K. S. Choudhary, "Designing intrusion detection to detect black hole and selective forwarding attack in wsn based on local information," in *ICCIT'09*, 2009, pp. 824–828.

[5] I. Khalil, S. Bagchi, C. N. Rotaru, and N. B. Shroff, "Unmask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks," *Ad Hoc Networks*, vol. 8, no. 2, pp. 148–164, 2010.

[6] E. C. H. Ngai, J. Liu, and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Comput. Commun.*, vol. 30, no. 11-12, pp. 2353–2364, 2007.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Mobicom'00*, 2000, pp. 255–265.

[8] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in *GLOBECOM'08*, 2008, pp. 1–5.

[9] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in wmns," *IEEE Trans. on Wireless Commun.*, vol. 9, no. 5, pp. 1661–1675, 2010.

[10] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify suspect nodes in selective forwarding attacks," *J. of Parallel and Distributed Computing*, vol. 67, pp. 1218–1230, 2007.

[11] K. Ren, W. Lou, and Y. Zhang, "Leds: Providing location-aware end-to-end data security in wireless sensor networks," *IEEE Trans. on Mobile Computing*, vol. 7, no. 5, pp. 585–598, 2008.

[12] J. Brown and X. Du, "Detection of selective forwarding attacks in heterogeneous sensor networks," in *ICC'08*, 2008, pp. 1583–1587.

[13] Y. Zhang, J. Yang, W. Li, L. Wang, and L. Jin, "An authentication scheme for locating compromised sensor nodes in wsns," *J. of Network and Comput. Applicat.*, vol. 33, no. 1, pp. 50–62, 2010.

[14] J. Sen and A. Ukil, "A secure routing protocol for wireless sensor networks," in *ICCSA 2010*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010, vol. 6018, pp. 277–290.

[15] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris, "Toward resilient routing in wireless sensor networks: Gradient-based routing in focus," in *SENSORCOMM'10*, 2010, pp. 478–483.

[16] F. L. Fessant, A. Papadimitriou, A. C. Viana, C. Sengul, and E. Palomar, "A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis," *Comput. Commun.*, vol. 35, no. 2, pp. 234–248, 2012.

[17] R. Machado and S. Tekinay, "A survey of game-theoretic approaches in wireless sensor networks," *Comput. Networks*, vol. 52, no. 16, pp. 3047–3061, 2008.

[18] A. Agah, K. Basu, and S. K. Das, "Security enforcement in wireless sensor networks: A framework based on non-cooperative games," *Pervasive and Mobile Computing*, vol. 2, no. 2, pp. 137–158, 2006.

[19] Y. B. Reddy and S. Srivathsan, "Game theory model for selective forward attacks in wireless sensor networks," in *MED'09*, 2009, pp. 458–463.

[20] V. V. V and V. M. A. Rajam, "Detection of colluding selective forwarding nodes in wireless mesh networks based on channel aware detection algorithm," *MES J. of Technology and Manage.*, pp. 62–66, 2011.

[21] S. Misra, P. V. Krishna, K. I. Abraham, N. Sasikumar, and S. Fredun, "An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks," *Comput. and Mathematics with Applicat.*, vol. 60, no. 2, pp. 294–306, 2010.

[22] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Secure high-throughput multicast routing in wireless mesh networks," *IEEE Trans. on Mobile Computing*, vol. 10, no. 5, pp. 653–668, 2011.

[23] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on manets," in *DNCMS'09*, 2009.

[24] S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in *WCECS'08*, 2008.

[25] P. S. Mogre, K. Graffi, M. Hollick, and R. Steinmetz, "A security framework for wireless mesh networks," *Wireless Commun. and Mobile Computing*, vol. 11, no. 3, pp. 371–391, 2011.

[26] S. Khan, K.-K. Loo, N. Mast, and T. Naeem, "Srpm: Secure routing protocol for ieee 802.11 infrastructure based wireless mesh networks," *J. Netw. Syst. Manage.*, vol. 18, no. 2, pp. 190–209, 2010.

[27] S. Khan and J. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks," *Wirel. Pers. Commun.*, vol. 62, no. 1, pp. 201–214, 2012.

[28] J. Eriksson, M. Faloutsos, and S. V. Krishnamurthy, "Routing amid colluding attackers," in *ICNP'07*, 2007, pp. 184–193.

[29] V. Toubiana, H. Labiod, L. Reynaud, and Y. Gourhant, "A global security architecture for operated hybrid wlan mesh networks," *Comput. Networks*, vol. 54, no. 2, pp. 218–230, 2010.

[30] I. Askoxylakis, B. Bencsáth, L. Buttyán, L. Dóra, V. Siris, D. Szili, and I. Vajda, "Securing multi-operator-based qos-aware mesh networks: requirements and design options," *Wireless Commun. and Mobile Computing*, vol. 10, no. 5, pp. 622–646, 2010.

[31] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," IETF RFC 3561, July 2003. [Online]. Available: http://tools.ietf.org/html/rfc3561

[32] M. Omar, Y. Challal, and A. Bouabdallah, "Certification-based trust models in mobile ad hoc networks: A survey and taxonomy," *J. of Network and Comput. Applicat.*, vol. 35, no. 1, p. 268C286, 2012.

[33] Y. Han, X. Gui, X. Wu, and X. Yang, "Proxy encryption based secure multicast in wireless mesh networks," *J. of Network and Comput. Applicat.*, vol. 34, no. 2, pp. 469–477, 2011.

[34] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, 2011.

[35] R. Azarderskhsh and A. Reyhani-Masoleh, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 2011, no. Article No. 16, p. 12 pages, 2011.

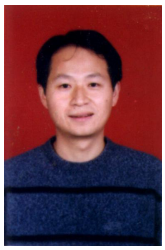
[36] P. Caballero-Gil and C. Hernández-Goya, "Efficient public key certificate management for mobile ad hoc networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 2011, no. Article No. 18, p. 11 pages, 2011.

[37] M. Nogueira, E. Silva, A. Santos, and L. Albini, "Survivable key management on wanets," *IEEE Wireless Commun.*, vol. 18, no. 6, pp. 82–88, 2011.
[38] M. Bellare and D. Micciancio, "A new paradigm for collision-free hashing: incrementality at reduced cost," in *EUROCRYPT'97*, 1997, pp. 163–192. [Online]. Available: http://dl.acm.org/citation.cfm?id=1754542.1754560
[39] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *Int. J. of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.
[40] J. Sen, *Applied Cryptography and Network Security*. Croatia: InTech, 2012.
[41] T. Clausen and P. Jacquet, "Optimized link state routing protocol (olsr)," IETF RFC 3626, October 2003. [Online]. Available: http://tools.ietf.org/html/rfc3626
[42] D. Eastlake and P. Jones, "Us secure hash algorithm 1 (sha1)," IETF RFC 3174, September 2001. [Online]. Available: http://tools.ietf.org/html/rfc3174
[43] V. R. Gandikota, B. R. Tamma, and C. S. R. Murthy, "Adaptive fec-based packet loss resilience scheme for supporting voice communication over ad hoc wireless networks," *IEEE Trans. on Mobile Computing*, vol. 7, no. 10, pp. 1184–1199, 2008.
[44] D. S. Moore, G. P. McCabe, and B. A. Craig, *Introduction to the Practice of Statistics*, 6th ed. New York, NY: W. H. Freeman and Company, 2007.
[45] R. Wrede and M. R. Spiegel, *Advanced Calculus*, 3rd ed. New York, NY: McGraw-Hill, 2010.

Qiang Liu received the B.S. and M.S. degrees from the National University of Defense Technology (NUDT) in 2007 and 2009, respectively. He is currently pursuing his Ph.D. degree in the School of Computer at NUDT. His research interests include protocol design and performance evaluation, Denial-of-Service detection as well as other security issues in wireless multi-hop networks.

Jianping Yin received the Ph.D. degree in computer science and technology from the National University of Defense Technology (NUDT) in 1990. He currently holds the positions of professor and the head of China Computer Federation Technical Committee on Theoretical Computer Science. His research interests include artificial intelligence, pattern recognition and network algorithm.

Victor C. M. Leung (S'75, M'89, SM'97, F'03) is a Professor of Electrical and Computer Engineering and holder of the TELUS Mobility Research Chair at the University of British Columbia (UBC). He has contributed some 600 technical papers, 25 book chapters and 5 book titles in the areas of wireless networks and mobile systems. He was a Distinguished Lecturer of the IEEE Communications Society. He has been serving on the editorial boards of the IEEE Transactions on Computers, IEEE Wireless Communications Letters and several other journals, and has contributed to the organizing and technical program committees of numerous conferences. Dr. Leung was a winner of the 2012 UBC Killam Research Prize, and the IEEE Vancouver Section Centennial Award. He is a Fellow of the Engineering Institute of Canada and the Canadian Academy of Engineering.



Zhiping Cai (M'08) received the Ph.D. degree in computer science and technology from the National University of Defense Technology (NUDT), Changsha, China, in 2005. He is now an associate professor of the School of Computer, NUDT. His current research interests include network security and network virtualization.