Malicious Link Detection in Multi-Hop Wireless Sensor Networks

Yuan Liang* Yunhao Liu† Jian Ren* Tongtong Li*
*Department of Electrical & Computer Engineering, Michigan State University
†Department of Computer Science & Engineering, Michigan State University
Email: liangy11@msu.edu, yunhao@cse.msu.edu, {renjian, tongli}@egr.msu.edu

***Abstract*—This paper considers malicious link detection in multi-hop wireless sensor networks (WSNs). Existing work on malicious link detection generally requires that the detection process being performed at the intermediate nodes, leading to considerable overhead in system design, as well as unstable detection accuracy due to limited resources and the uncertainty in the loyalty of the intermediate nodes themselves. In this paper, we propose an efficient and robust malicious link detection scheme by exploiting the statistics of packet delivery rates only at the base station. More specifically, first, we present a secure packet transmission protocol to ensure that except the base station, any intermediate nodes on the route cannot access the contents and routing paths of the packets. Second, we design a malicious link detection algorithm that can effectively detect the irregular dropout at every hop (or link) along the routing path. We prove that the proposed algorithm has guaranteed false alarm rate and low miss detection rate. Simulation results are provided to validate the proposed approaches.**

I. Introduction

Wireless sensor networks (WSNs) are often multi-hop networks where individual sensor nodes need to function as relays to forward the data flow originated from their peers to the sink. Such a distributed network organization makes WSNs especially vulnerable to various attacks, such as wireless jamming, spoofing attacks and internal attacks [1], in a sense that one malicious link or node in the network can compromise the data flow passing through it from multiple nodes. In this paper, we consider the detection of malicious links in WSNs.

The detection of malicious behaviors in WSNs, or more generally, the multi-hop wireless networks, has been broadly discussed in literature. In [2], [3], audit based schemes were proposed for malicious node identification. In [4], the security of disruption tolerant networks (DTN) was studied. In [5], an heuristic method was proposed to identify the failed nodes by re-organizing the network topology. In [6], a 2ACK scheme was proposed to detect the nodes that intentionally drop packets. In [7], the blackhole and grayhole attacks were investigated. In [8], the malicious node detection was explained under the context of network coding. Making use of the open medium in wireless communications, an overhearing scheme was proposed to monitor the behaviors of the neighboring nodes in [9].

This paper is partially supported by the National Science Foundation under awards ECCS-1744604, CCF-1919154 and ECCS-1923409.

A major limitation with most existing methods on malicious behavior detection is that the nodes are required to implement additional verification process in packet delivery, or report additional information to the authority in the network, leading to considerable overhead on complexity, energy consumption and throughput. In this paper, as an effort to improve the efficiency and minimize the system complexity, we propose a malicious link detection algorithm by exploiting the statistics of packet delivery rates at the base station. More specifically, first, we present a secure packet transmission protocol to ensure that except the base station, any intermediate nodes on the route cannot access the contents and routing paths of the packets. Second, we design a malicious link detection algorithm that can effectively detect the irregular dropout at *every hop (or link)* along the routing path with guaranteed false alarm rate and miss detection rate. Comparing to [10] which can detect whether a routing path is problematic, our detection method can be localized to every link. It should be pointed out that, illegal packet modification and injection of invalid packets, which essentially result in the dropout of legal packets, can be detected successfully as well. Simulation results are provided to validate the proposed approaches.

II. Network Model

In this paper, we consider a single unit of a multi-hop WSN. The unit is governed by an authority, the sink or the base station (BS), which is responsible for collecting data from the nodes in the unit, and issuing control messages. Each node can be either a regular sensor or the aggregator of several sensors. In this paper, we model the WSN unit using the N-hop framework [11], as shown in Fig. 1, where the nodes are sorted basing on the hop distance from each node to the BS. The nodes on layer i are the set of nodes i hops away from the BS; each node at layer $i+1$ forwards the packets it generates and receives from higher layers to one or several nodes at layer i until the BS (layer 0). The proposed scheme can be readily scalable to WSNs with multiple BSs.

In a WSN, the major data flow is from the sensors to the base station, i.e., the uplink. Therefore, in this paper, we focus on the uplink data flow of the WSN. Since we consider an environment where the reliability of the links cannot be guaranteed, we employ multi-path routing [12] in the network, to enhance the diversity and robustness of routing. For each packet to be delivered to the BS, a node randomly selects

978-1-7281-0962-6/19/$31.00 ©2019 IEEE

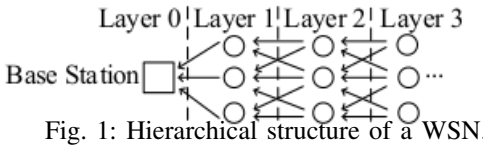


Fig. 1: Hierarchical structure of a WSN.

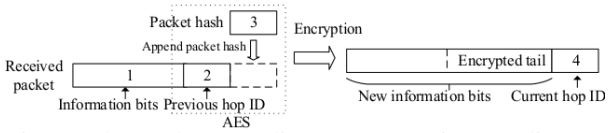


Fig. 2: The packet encoding process at intermediate node.

one of the candidate nodes in the lower layer as the next hop with certain probability according to the routing table; the routing table is determined by the BS and assigned to each node through the control message. The topology and the routing table of the network can be determined either statically or dynamically. In the static case, the topology and routing paths are essentially fixed during network operation. In the dynamic case, the routing table can be determined by utilizing the ad-hoc on-demand distance vector (AODV) routing [13] protocol, where the BS sorts the route request (RREQ) messages and selects the next hops accordingly for each node in the unit. Since the major focus of this paper is on malicious link detection process, in the following, we assume that the routing table has been established and fixed during detection.

The malicious behaviors considered in this paper include (i) irregular dropout of packets, (ii) illegal modification of packets, and (iii) injection of invalid packets. The reasons for the malicious behaviors may be the degradation of wireless channels, attacks from external jammers or corrupted internal nodes, etc. Note that the above malicious behaviors committed by an internal node can be equivalently converted to those happen on its incidental links; therefore, without loss of generality we focus on malicious link detection. A node can be considered as malicious if a certain amount of its incidental links are identified as malicious. We will further show in Section III that the detection of packet modification and packet injection can both be converted to that of packet dropout.

Notations: We let N_i denote the number of node of layer i. Following the notation in graph theory, the nodes of layer i are denoted by $v_{i,0}, v_{i,1}, ..., v_{i,N_i-1}$, and $v_{0,0}$ denotes the BS; e_{i,j_1,j_2} denotes the link/edge $v_{i,j_1} \rightarrow v_{i-1,j_2}$. $G_{i,j}$ denotes the self generated packet rate of node $v_{i,j}$, $p_d(i,j_1,j_2)$ the dropout rate of link e_{i,j_1,j_2}, $p_t(i,j_1,j_2)$ the probability that v_{i,j_1} selects v_{i-1,j_2} as its next hop in the multi-path routing. $\mathbb{F}_q^n$ denotes the Galois Field (q^n). We use bold capital letters, e.g., $\boldsymbol{X}$, to denote random vectors, and bold lower case letters, e.g., $\boldsymbol{x}$, to denote their values.

III. Packet Transmission Protocol

In this section, we design the packet transmission protocol for the WSN. In order to combat packet content attacks, we encrypt the transmitted packets so that except the BS, any intermediate nodes on the route cannot access the contents and the paths of the packets. However, it should be noted that the proposed protocol is not necessary in malicious link detection if the malicious party does not launch attacks basing on the packet contents.

A. Protocol Description

1) Packet Encoding: Each node in the WSN shares a distinct secret key with the BS for packet encryption. Each packet received at a node contains two parts: the information bits and the ID of the previous hop. Let the length of the node ID be L_n bits. In addition to the content generated from the source, the information bits also contain the history of the previous hops the packet passed through, however, that information is encrypted by each previous hop so it is not accessible by the current node. The encoding process in packet forwarding includes the following steps:

- Generate a packet hash and append it to the packet. The hash is calculated using the entire packet based on a secure hash algorithm [14]. The secure hash is inserted to provide integrity check of the packet. For efficiency, the generated hash sequence may be truncated before attached to the packet. Let the length of the hash sequence be L_h bits.
- Encrypt the tail part of the packet, including the previous hop ID and packet hash. In general, the verification of a packet is implemented by certain asymmetric encryption algorithms [14]. However, since only the BS, rather than the intermediate nodes, is required to check the integrity of the received packet; hence a symmetric block cipher, i.e., AES algorithm, is sufficient in the proposed scheme. In practice, if the length of the tail, $L_t = L_n + L_h$, is less than, or not a multiple of the block size of AES cipher, we can include the tail of the information bits in the plain text.
- Append the node ID to the packet and transmit it to the next hop.

The encoding process is demonstrated in Fig. 2. The proposed packet relaying protocol ensures that each packet is not traceable in delivery. Therefore, the malicious party is unable to launch attacks to packets based on the routing history.

2) Packet Decoding at the BS: At the reception of a packet, the BS applies the inverse of the encoding process successively. Suppose the BS has recovered the packet received at node v_{i-1,j_2}, and found that the previous hop is v_{i,j_1} basing on the tail of the packet. Then by decrypting the tail part of the information bits, the BS obtains the packet hash, as well as the packet received by node v_{i,j_1}. Since the BS stores the secret keys of all the nodes in the network, it is able to recover the packet version received by each intermediate node on the route if no malicious link exists.

3) Protocol Implementation and Efficiency: The proposed protocol is implemented between the existing network layer and transmission layer of the WSN. This implementation has

two advantages: first, it facilitates easy integration into any existing systems; second, the packet length in the proposed protocol is not limited by the network layer design. Therefore, the loss of throughput from the appended tails at the intermediate nodes can be leveraged by the increased packet length.

B. Security Analysis

In this subsection, we first discuss the security of the packet transmission scheme under illegal packet modification, then we show that both the detection of packet modification and injection can be converted to that of the packet dropout.

Suppose e_{i,j_1,j_2} is a malicious link in the network and the secret key of v_{i,j_1} is unknown to the malicious party. For an arbitrary packet passing through e_{i,j_1,j_2}, let $\boldsymbol{X}_{i,j_1,j_2} \in \mathbb{F}_2^L$ denote the vector of its information bits and $\boldsymbol{E}_{i,j_1,j_2} \in \mathbb{F}_2^L$ the error pattern applied on it, where L is the length of the information bits. To modify the packet without being detected, the malicious link seeks an error pattern $\boldsymbol{E}_{i,j_1,j_2} \neq \boldsymbol{0}$ such that $\boldsymbol{Y}_{i,j_1,j_2} = \boldsymbol{X}_{i,j_1,j_2} + \boldsymbol{E}_{i,j_1,j_2}$ is a valid output of v_{i,j_1}. We have the following proposition on the security.

Proposition 1. *Assuming an ideal cipher (random oracle), the probability that the malicious link generates an unseen $\boldsymbol{Y}_{i,j_1,j_2}$ that is valid is negligible if it is infeasible for the malicious party to succeed in the preimage attack to the hash function.*

Proof. Let $f(\cdot)$ denote the encryption function, which is an bijective mapping defined on $\mathbb{F}_2^{L_t} \mapsto \mathbb{F}_2^{L_t}$. For the random oracle, if the secret key is unknown, for any integer $1 \leq m \leq 2^{L_t}$ and $\boldsymbol{x} \in \mathbb{F}_2^{L_t}$, we have

$$\begin{aligned} &\Pr\{f(\boldsymbol{x}) = \boldsymbol{y} \mid f(\boldsymbol{x}_k) = \boldsymbol{y}_k, 1 \leq k \leq m\} \\ &= \begin{cases} \frac{1}{2^{L_t}-m}, & \boldsymbol{y} \in \mathbb{F}_2^{L_t},\ \boldsymbol{y} \notin \{\boldsymbol{y}_k \mid 1 \leq k \leq m\}, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{1}$$

where for $1 \leq k \leq m$, $\boldsymbol{x}_k \in \mathbb{F}_2^{L_t}$ and $\boldsymbol{x} \neq \boldsymbol{x}_k$. That is, the cipher text of an unseen plain text is uniformly distributed over all the unseen cipher texts, and vice versa. For the encrypted tail with error $\boldsymbol{Y}_{i,j_1,j_2}(L - L_t :)$, we consider two cases:

First, if $\boldsymbol{Y}_{i,j_1,j_2}(L - L_t :)$ has been seen, i.e., the malicious link uses the encrypted tail of another packet to replace the current packet; let $f(\boldsymbol{X}') = \boldsymbol{Y}_{i,j_1,j_2}(L - L_t :)$, then the target of the malicious party is to find a vector $\boldsymbol{Y}_{i,j_1,j_2}(: L - L_t)$, combined with $\boldsymbol{X}'(: L_t - L_h)$, such that its hash value is $\boldsymbol{X}'(L_t - L_h :)$. This is the preimage attack to the hash function.

Second, if $\boldsymbol{Y}_{i,j_1,j_2}(L - L_t :)$ has not been seen before, then for the malicious party, the plain text of $\boldsymbol{Y}_{i,j_1,j_2}(L - L_t :)$ is uniformly distributed over all the unseen plain texts. For any given prefix vector $\boldsymbol{Y}_{i,j_1,j_2}(: L - L_t)$, there are $2^{L_t - L_h}$ possible tails since the hash value is determined by the content; so given m observed plain and cipher texts for $f(\cdot)$, the probability that $\boldsymbol{Y}_{i,j_1,j_2}$ is valid is $\frac{2^{L_t-L_h}}{2^{L_t}-m} \approx \frac{1}{2^{L_h}}$, which is negligible for a large L_h. □

A secure hash function which is believed to be resistant against preimage attacks generally requires L_h to be more than 256 bits [15]. However, considering the efficiency, such hash value might be too long since each hop attaches a hash to the packet in relaying. So we employ two different policies depending on the power of malicious party:

Case I: If the malicious party is unable to attack the hash function at each hop, then we believe $\boldsymbol{E}_{i,j_1,j_2} = \boldsymbol{0}$ if $\boldsymbol{Y}_{i,j_1,j_2}$ passes the verification. In this case, for each packet, we are able to locate the last misbehaved link on the route if any.

Case II: If the malicious party is able to attack the hash function at each hop, then $\boldsymbol{E}_{i,j_1,j_2}$ might be non-zero even if $\boldsymbol{Y}_{i,j_1,j_2}$ passes the verification. However, while the BS is unable to locate the misbehaved link, it is still able to detect an error by checking the integrity of the packet content. In this case, the BS drops the packet.

For generality, in the following analysis, we focus on case II, where the hash can be quite short to achieve higher efficiency. However, case I provides a quick identification of malicious links for illegal packet modification, when the malicious party is less powerful.

Next, we show that the detection of packet modification and injection can be converted to that of legitimate packet dropout.

Packet Modification: As is noted in case II, the modified packets can be detected by checking the packet contents at the BS. This requires the encryption and verification on the higher layers, e.g., the application layer, which has less effect on the efficiency as they are applied only by the source node. The modified packets will be dropped by the BS, which is equivalent to the packet dropout on the malicious link.

Packet Injection: To prevent the injection of invalid packets in the WSN, e.g., the denial of service (DoS) attacks, we apply flow control at each node for each incoming link. Because of the flow control, the invalid packets will occupy the resources of the legitimate packets on the same link, and again, the legitimate packets will be dropped on the malicious link.

IV. The Proposed Malicious Link Detection Algorithm

In this section, we present the proposed malicious link detection algorithm. As shown in Section III, the malicious behaviors considered in this paper can be converted to the irregular packet dropout on the malicious links. The proposed algorithm hence detects links with higher dropout rate than a predefined baseline, denoted by p_0. Our algorithm relies solely on the statistics of packet delivery at the BS to identify the malicious links, and does not require any additional information collected from the nodes. Therefore, the system complexity and overhead can be kept minimum.

We will analyze the packet delivery ratio of each node in the WSN during an observation window. We assume the duration of the observation window is T. $K_{i,j}$ denotes number of received packets at BS generated by $v_{i,j}$ during the observation window, while K_{i,j_1,j_2} denotes number of received packets generated by v_{i,j_1} and passing through e_{i,j_1,j_2} during the observation window.

In the following, we first consider the simplistic case of a 1-hop network, then we discuss the 2-hop network, and further generalize the algorithm to the N-hop network. Finally, we analyze the misdetection rate of the proposed algorithm.

A. 1-Hop Network

The nodes in 1-hop network connect to the BS directly. Verifying the dropout rate of link $e_{1,j,0}$ can be formulated as a one-tailed hypothesis testing on a Bernoulli random variable (RV) as

$$\text{Null hypothesis } H_0 : p_d(1,j,0) \le p_0.$$
$$\text{Alternative hypothesis } H_1 : p_d(1,j,0) > p_0.$$

During the observation window of the algorithm, the number of packets generated from $v_{1,j}$ can be approximated by $\lfloor TG_{1,j} \rfloor$. $K_{1,j}$ should follow a binomial distribution $B(\lfloor TG_{1,j} \rfloor, 1 - p_d(1,j,0))$. Conventionally, by allowing a probability of α to reject a true hypothesis (type I error or false alarm), define threshold $\theta(\alpha)$ as

$$\theta(\alpha, n, p) \triangleq \max\left\{\theta \mid \sum_{k=0}^{\theta} \binom{n}{k} (1-p)^k p^{n-k} \le \alpha\right\}. \quad (2)$$

Then we reject hypothesis H_0 if $K_{1,j} < \theta(\alpha, \lfloor TG_{1,j} \rfloor, p_0)$ in the observation window, i.e., link $e_{1,j,0}$ is identified as malicious.

B. 2-Hop Network

In a 2-hop network, all the links incidental to the BS can be tested as in the 1-hop network. Here we focus on the links between layer 2 and layer 1, e.g., e_{2,j_1,j_2}. We test the following hypothesis:

$$\text{Null hypothesis } H_0 : p_d(2,j_1,j_2) \le p_0. \quad (3)$$
$$\text{Alternative hypothesis } H_1 : p_d(2,j_1,j_2) > p_0. \quad (4)$$

With multi-path routing, the data rate on e_{2,j_1,j_2} is $p_t(2,j_1,j_2)G_{2,j_1}$. Since the contents and path information of each packet are encrypted, all the packets generated by v_{2,j_1} and received by v_{1,j_2} should be treated equivalently as the packets generated by v_{1,j_2} after leaving v_{1,j_2}[1]. Let $p_d(1,j_2)$ denote the dropout rate of the combined path from v_{1,j_2} to BS. Hence, K_{2,j_1,j_2} follows a binomial distribution $B(\lfloor Tp_t(2,j_1,j_2)G_{2,j_1} \rfloor, (1 - p_d(2,j_1,j_2))(1 - p_d(1,j_2)))$, while K_{1,j_2} follows a binomial distribution $B(\lfloor TG_{1,j_2} \rfloor, (1 - p_d(1,j_2)))$. However, we are unable to apply the algorithm in the 1-hop network directly to testing link e_{2,j_1,j_2} as $p_d(1,j_2)$ is unknown. Even if we can obtain an estimate of $p_d(1,j_2)$ from the value of K_{1,j_2}, the estimation error would render the false alarm rate unbounded, as will be shown in Section V.

We solve the problem by exploiting the joint distribution of K_{2,j_1,j_2} and K_{1,j_2}, where we derive a bounded false alarm in testing e_{2,j_1,j_2}. The result is generalized in the following proposition.

Proposition 2. *Consider i.i.d RVs $X_i \sim Bernoulli(p), i = 1,...,n_1$ and $Y_i \sim Bernoulli(pq), i = 1,...,n_2$, $p \in (0,1), q \in (0,1)$. Let $X = \sum_i X_i$ and $Y = \sum_i Y_i$ follow binomial distribution $B(n_1,p)$ and $B(n_2,pq)$, respectively, and $\Phi(x;n,\rho)$ denote the distribution function of binomial distribution $B(n,\rho)$, i.e.*

$$\Pr\{X = x\} = \Phi(x;n_1,p), \quad \Pr\{Y = y\} = \Phi(y;n_2,pq). \quad (5)$$

For any $\alpha \in (0,1)$, $n \in \mathbb{Z}^+$ and $x \in (0,\infty)$, define $\rho(\alpha,n,x)$

$$\rho(\alpha,n,x) \triangleq \max\{\rho \mid \sum_{k=\lceil x \rceil}^{n} \Phi(k;n,\rho) \le \alpha, \rho \in [0,1]\}, \quad (6)$$

and define $\theta(\alpha,m,n,q,x) \in \mathbb{Z}^+$ as

$$\theta(\alpha,m,n,q,x) \triangleq \max\{\theta \mid \sum_{k=0}^{\theta} \Phi(k;n,\rho(\alpha,m,x)q) \le \alpha\}, \quad (7)$$

then for $\alpha \in (0,1)$ we have

$$P_{false} = \Pr\{Y \le \theta(\alpha,n_1,n_2,q,X)\} \le 2\alpha. \quad (8)$$

Proof. For $\rho \in [0,1]$, $n \in \mathbb{Z}^+, \alpha \in (0,1)$, we define function

$$x(n,\rho,\alpha) = \min\{x \mid \sum_{k=x}^{n} \Phi(k;n,\rho) \le \alpha, x \in \mathbb{Z}^+\}, \quad (9)$$

e.g. $\Pr\{X \ge x(n_1,p,\alpha)\} \le \alpha$ and $\Pr\{X \ge x(n_1,p,\alpha) - 1\} > \alpha$. Note that for any fixed $x \in (0,\infty)$ and $n \in \mathbb{Z}^+$, function $\sum_{k=\lceil x \rceil}^{n} \Phi(k;n,\rho)$ is non-decreasing w.r.t. $\rho \in [0,1]$. Then we have

$$\rho(\alpha,n,x(n,\rho_0,\alpha) - 1) < \rho_0, \ \rho_0 \in (0,1). \quad (10)$$

which can be obtained from the fact that $\sum_{k=x(n,\rho_0,\alpha)-1}^{n} \Phi(k;n,\rho_0) > \alpha$.

From the monotonicity of $\sum_{k=\lceil x \rceil}^{n} \Phi(k;n,\rho)$, we have

$$\sum_{k=0}^{\theta(\alpha,m,n,q,x(m,\rho_0,\alpha)-1)} \Phi(k;n,\rho_0 q) \le \alpha. \quad (11)$$

Also note that for any fixed $\alpha \in (0,1)$ and $n \in \mathbb{Z}^+$, $\rho(\alpha,n,x)$ is non-decreasing w.r.t. $x \in (0,\infty)$. Again, using the monotonicity of $\sum_{k=\lceil x \rceil}^{n} \Phi(k;n,\rho)$, $\theta(\alpha,m,n,q,x)$ is non-decreasing w.r.t. $x \in (0,\infty)$ with other parameters being fixed. According to (9) and (11) and the fact that X and Y are independent, we have

$$\begin{aligned} P_{false} &= \sum_{x=0}^{n_1} \Pr\{X = x\} \Pr\{Y \le \theta(\alpha,n_1,n_2,q,x)\} \\ &\le \alpha + \Pr\{Y \le \theta(\alpha,n_1,n_2,q,x(n_1,p,\alpha) - 1)\}, \end{aligned} \quad (12)$$

where $\Pr\{Y \le \theta(\alpha,n_1,n_2,q,x(n_1,p,\alpha) - 1)\}$ equals

$$\sum_{k=0}^{\theta(\alpha,n_1,n_2,q,x(n_1,p,\alpha)-1)} \Phi(k;n_2,pq) \le \alpha. \quad (13)$$

which completes the proof. □

According to Proposition 2, by setting the threshold of K_{2,j_1,j_2} as $\theta(\alpha, \lfloor TG_{1,j_2} \rfloor, \lfloor Tp_t(2,j_1,j_2)G_{2,j_1} \rfloor, 1 - p_0, K_{1,j_2})$, the false alarm rate in testing is upper bounded by 2α. In this way, all the links can be tested.

[1]It is possible that v_{1,j_2} treats the packets it relays and those it generates differently, however, since the malicious node behavior can be considered as that of its incidental links, i.e., e_{2,j_1,j_2}, this will not void the results of the detection algorithm.

C. N-hop Network

We further generalize the algorithm to the N-hop network. Consider link $e_{i,j_1,j_2}, i > 1$ in the network. The input data rate originated from v_{i,j_1} on e_{i,j_1,j_2} is $p_t(i,j_1,j_2)G_{i,j_1}$; after being received by v_{i-1,j_2}, these packets should have the same routing distribution as those originated from v_{i-1,j_2} if v_{i-1,j_2} behaves normally. Let $p_d(i-1,j_2)$ denote the dropout rate from v_{i-1,j_2} to BS. Then both K_{i,j_1,j_2} and K_{i-1,j_2} follow binomial distributions. According to Proposition 2, if $K_{i,j_1,j_2} \leq \theta(\alpha, \lfloor TG_{i-1,j_2} \rfloor, \lfloor Tp_t(i,j_1,j_2)G_{i,j_1} \rfloor, 1-p_0, K_{i-1,j_2})$, we identify e_{i,j_1,j_2} as malicious, whose false alarm rate is bounded by 2α.

It is possible that v_{i-1,j_2} may treat the packets it relays differently from those it generates, e.g., dropping the incoming packets or forwarding them disobeying the routing table. These malicious behaviors can be decomposed as either the dropout on the incoming links or the injection to the outgoing links, which can both be detected by the proposed algorithm as noted in Section III. Therefore, the misbehavior of v_{i-1,j_2} will not void the generality of the proposed algorithm.

D. Misdetection Rate Analysis

In this subsection, we show that in the proposed algorithm, if the dropout rate from the end node to the BS is less than 1, the misdetection rate on a link converges to 0 as $T \to \infty$.

Misdetection happens on link e_{i,j_1,j_2} if its dropout rate $p_d(i,j_1,j_2)$ is greater than the base line p_0 while K_{i,j_1,j_2} and K_{i-1,j_2} satisfy $K_{i,j_1,j_2} > \theta(\alpha, \lfloor TG_{i-1,j_2} \rfloor, \lfloor Tp_t(i,j_1,j_2)G_{i,j_1} \rfloor, 1-p_0, K_{i-1,j_2})$. The analysis on the probability is summarized in the following proposition.

Proposition 3. *Consider i.i.d RVs $X_i \sim Bernoulli(p), i = 1,...,n_1$ and $Y_i \sim Bernoulli(pq), i = 1,...,n_2$, $p \in (0,1], q \in (0,1)$. Let $X = \sum_i X_i$ and $Y = \sum_i Y_i$ follow binomial distribution $B(n_1,p)$ and $B(n_2,pq)$, respectively, and suppose $n_2/n_1 = \kappa$ being fixed. For some $\hat{q} > q$, the probability that $Y > \theta(\alpha, n_1, n_2, \hat{q}, X)$ converges to 0 as $n_2 \to +\infty$. More specifically, as $n_2 \to +\infty$, the miss detection rate $P_{miss} = \Pr\{Y > \theta(\alpha, n_1, n_2, \hat{q}, X)\}$ satisfies*

$$P_{miss} \leq \left[\frac{e^{(1-\delta)\hat{q}/q-1}}{[(1-\delta)\hat{q}/q]^{(1-\delta)\hat{q}/q}} + o(1) \right]^{n_2 pq} + e^{-\frac{\delta}{2} n_1 p}, \quad (14)$$

for any $\delta \in (0,1)$ and $(1-\delta)\hat{q}/q > 1$.

Proof. Note that X and Y are independent, so are $\theta(\alpha, n_1, n_2, \hat{q}, X)$ and Y. Therefore, the misdetection rate can be expressed as

$$P_{miss} = \sum_{x=0}^{n_1} \Phi(x; n_1, p) \sum_{y=\theta(\alpha,n_1,n_2,\hat{q},x)+1}^{n_2} \Phi(y; n_2, pq). \quad (15)$$

One Chernoff bound of binomial distribution $B(n,\rho)$ is

$$\sum_{k=\lceil x \rceil}^{n} \Phi(k; n, \rho) \leq \frac{(n\rho)^x e^{x-n\rho}}{x^x}. \quad (16)$$

for $x \geq n\rho$. This implies a lower bound of $\rho(\alpha, n, x)$ is

$$\rho(\alpha, n, x) \geq -\frac{x}{n} W_0(-\frac{\alpha^{\frac{1}{x}}}{e}). \quad (17)$$

where $W_0(\cdot)$ is the principle branch of the Lambert W function.

Another Chernoff bound of the binomial distribution is

$$\sum_{k=0}^{\theta} \Phi(k; n, \rho) \leq e^{-\frac{(n\rho-\theta)^2}{2n\rho}}, \quad (18)$$

for $\theta \leq n\rho$, from which we have a lower bound of (2) as

$$\theta(\alpha, n, \rho) \geq n\rho - \sqrt{-2n\rho \log \alpha}. \quad (19)$$

Note that $\sum_{k=0}^{\theta} \Phi(k; n, \rho)$ is non-increasing w.r.t. ρ with other parameters being fixed. From (17), we obtain a lower bound of $\theta(\alpha, m, n, q, x)$ as

$$-\frac{n}{m} x W_0(-\frac{\alpha^{\frac{1}{x}}}{e}) q - \sqrt{2\frac{n}{m} x W_0(-\frac{\alpha^{\frac{1}{x}}}{e}) q \log \alpha}, \quad (20)$$

where we denote (20) by $\tilde{\theta}(\alpha, m, n, q, x)$.

Since $\theta(\alpha, m, n, q, x)$ is non-decreasing w.r.t. x, for any $x_0 \in [0, n_1]$, an upper bound of P_{miss} is given by

$$P_{miss} \leq \Pr\{X \leq x_0\} + \Pr\{Y \geq \theta(\alpha, n_1, n_2, \hat{q}, x_0)\}. \quad (21)$$

Let $x_0 = (1-\delta)n_1 p$ for some $\delta \in (0,1)$ and $n_2/n_1 = \kappa$ being fixed, then we have

$$\lim_{n_1 \to +\infty} \frac{\tilde{\theta}(\alpha, n_1, n_2, \hat{q}, x_0)}{n_1} = (1-\delta)\kappa p \hat{q}, \quad (22)$$

i.e., $\tilde{\theta}(\alpha, n_1, n_2, \hat{q}, x_0) = (1-\delta)n_2 p\hat{q} + o(n_1)$. Since $q < \hat{q}$, by setting δ such that $1 - \delta > q/\hat{q}$, we can derive an upper bound of $\Pr\{Y \geq \theta(\alpha, n_1, n_2, \hat{q}, x_0)\}$ from (16) and (20) as

$$\left[\frac{e^{(1-\delta)\hat{q}/q-1+o(n_1)/n_2}}{[(1-\delta)\hat{q}/q + o(n_1)/n_2]^{(1-\delta)\hat{q}/q+o(n_1)/n_2}} \right]^{n_2 pq}. \quad (23)$$

As $n_2 \to +\infty$, the (23) can be rewritten as

$$\left[\frac{e^{(1-\delta)\hat{q}/q-1}}{[(1-\delta)\hat{q}/q]^{(1-\delta)\hat{q}/q}} + o(1) \right]^{n_2 pq}, \quad (24)$$

where $\frac{e^{(1-\delta)\hat{q}/q-1}}{[(1-\delta)\hat{q}/q]^{(1-\delta)\hat{q}/q}} \in (\frac{e^{\hat{q}/q-1}}{(\hat{q}/q)^{\hat{q}/q}}, 1)$. Furthermore, from (18),

$$\Pr\{X \leq x_0\} \leq e^{-\frac{\delta}{2} n_1 p}. \quad (25)$$

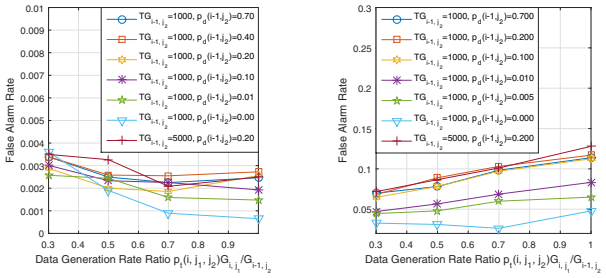
Then (15) follows from (21), (24) and (25), which completes the proof. □

V. Simulation

In this section, we validate the the proposed malicious link detection algorithm through numerical examples.

We consider an arbitrary link e_{i,j_1,j_2} during an observation window of duration T. To demonstrate the performance of the proposed algorithm under different network settings, we vary the data rates G_{i,j_1} and G_{i-1,j_2}, the dropout rates $p_d(i,j_1,j_2)$ and $p_d(i-1,j_2)$, in the numerical results.

Baseline Algorithm: Since the difficulty of the malicious link detection lies in that the dropout rate $p_d(i-1,j_2)$ is



(a) Proposed algorithm (b) Baseline algorithm

Fig. 3: The false alarm rates versus the data generation rate ratio $p_t(i,j_1,j_2)G_{i,j_1}/G_{i-1,j_2}$.

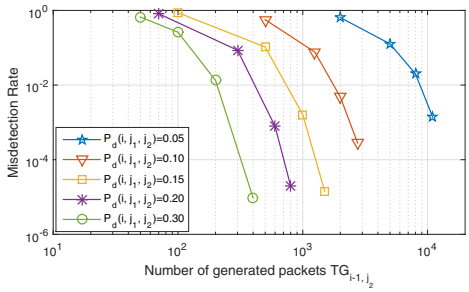


Fig. 4: The misdetection rate of the proposed algorithm versus the number of generated packets in the observation window TG_{i-1,j_2} for $p_d(i-1,j_2)=0.2$ and $\frac{p_t(i,j_1,j_2)G_{i,j_1}}{G_{i-1,j_2}}=1$.

unknown at the BS, we consider a baseline algorithm which first estimates $p_d(i-1,j_2)$ by

$$\tilde{p}_d = K_{i-1,j_2}/(TG_{i-1,j_2}). \tag{26}$$

Then for a baseline dropout rate p_0, it calculates the threshold in the hypothesis test following the traditional method by

$$\theta(\alpha, Tp_t(i,j_1,j_2)G_{i,j_1}, (1-\tilde{p}_d)(1-p_0)), \tag{27}$$

for an allowed false alarm rate of α. However, we will see that its actual false alarm rate cannot be bounded by α.

False alarm rate comparison between the proposed algorithm and the baseline algorithm: In this example, we set the allowed false alarm rate $\alpha_0 = 0.05$ and the baseline dropout rate as $p_0 = p_d(i,j_1,j_2) = 0.01$. The results are plotted in Fig. 3a and Fig. 3b, respectively. For the proposed algorithm, it is shown the actual false alarm rate is much lower than the required bound α_0. On the other hand, because of the error in $p_d(i-1,j_2)$ estimation, the baseline algorithm cannot bound the false alarm rate in detection unless the dropout rate $p_d(i-1,j_2)$ is very close to 0.

Misdetection rate of the proposed algorithm: In this example, we evaluate the misdetection rate of the proposed algorithm when e_{i,j_1,j_2} is a malicious link. We keep the baseline dropout rate $p_0 = 0.01$ and false alarm rate upper bound $\alpha_0 = 0.05$, and set $p_t(i,j_1,j_2)G_{i,j_1}/G_{i-1,j_2} = 1$ and $p_d(i-1,j_2) = 0.2$. The results are plotted in Fig. 4. The numerical results are consistent with the theoretical analysis, i.e., the misdetection rate becomes arbitrarily small as the observation window duration T increases. However, the number of packets needed for an accurate detection varies significantly with the actual dropout rate $p_d(i,j_1,j_2)$.

VI. Conclusion

In this paper, we proposed an efficient and robust malicious link detection scheme for multi-hop WSNs. Comparing with existing approaches that rely on the intermediate nodes to carry out the detection process, in the proposed scheme, malicious link detection was only performed at the base stations by exploiting the statistics of packet delivery rates. As a result, the proposed scheme could effectively detect the irregular dropout at every hop (or link) along the routing paths with significantly higher accuracy, and at the same time, reducing system overhead and improving the efficiency. The effectiveness of the proposed scheme was demonstrated through both theoretical analysis and simulation results.

References

[1] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys Tutorials*, vol. 11, no. 2, pp. 52–73, Second 2009.

[2] Y. Zhang, L. Lazos, and W. Kozma, "Amd: Audit-based misbehavior detection in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 8, pp. 1893–1907, Aug 2016.

[3] T. Shu and M. Krunz, "Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 813–828, April 2015.

[4] Q. Li and G. Cao, "Mitigating routing misbehavior in disruption tolerant networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 664–675, April 2012.

[5] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *Proceedings of ACM International Workshop on Wireless Sensor Networks and Applications*, 2002, pp. 122–130.

[6] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536–550, May 2007.

[7] J. Chang, P. Tsou, I. Woungang, H. Chao, and C. Lai, "Defending against collaborative attacks by malicious nodes in manets: A cooperative bait detection approach," *IEEE Systems Journal*, vol. 9, no. 1, pp. 65–75, March 2015.

[8] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "Mis: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in *Proceedings of IEEE INFOCOM*, March 2010, pp. 1–5.

[9] S. Buchegger and J. . L. Boudec, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Communications Magazine*, vol. 43, no. 7, pp. 101–107, July 2005.

[10] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Personal Communications*, vol. 29, no. 3, pp. 367–388, Jun 2004.

[11] T. Li, M. Abdelhakim, and J. Ren, "N-hop networks: A general framework for wireless systems," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 98–105, 2014.

[12] D. Thaler and C. Hopps, "Multipath issues in unicast and multicast next-hop selection," United States, 2000.

[13] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, Feb 1999, pp. 90–100.

[14] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman & Hall/CRC, 2007.

[15] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in *International Workshop on Fast Software Encryption*, 2004, pp. 371–388.