Detecting Link Correlation Spoofing Attack: A Beacon-Trap Approach

Hang Shen, Jiajia Xu, Tianjing Wang, Guangwei Bai
College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China
{hshen, xujiajia, wangtianjing, bai}@njtech.edu.cn

***Abstract*—Incorporating link correlation awareness into wireless network protocols to facilitate data transmission is an important research issue. In this paper, we focus on link correlation based security threat and countermeasure in wireless networks. By taking advantage of the vulnerability of beacon-based link correlation measurement and the blind spot of malicious node detection mechanisms, we design a new type of link correlation spoofing attack (LCSA) to decrease protocol performance by distorting link correlation information while escaping the tracking of any watchdog and trust systems. Typical cases are analyzed to quantify how the LCSA covertly weakens protocol performance. We also propose beacon-trap (BT), a countermeasure embedded in the beacon-based link condition measurement protocol. Using link diversity as a cover, BT sets traps in the beacon sending sequence to ambush malicious nodes that launch LCSAs without extra control overhead. The performance of BT is not affected by changes in the size of a network or the distribution of nodes. Numerical results demonstrate the superiority and effectiveness of BT against LCSAs in terms of malicious node detection success rate and speed under different parameter settings.**

***Index Terms*—link correlation spoofing attack, beacon-based measurement, trap, detection success rate, wireless networks**

I. Introduction

RECENT studies show that packet receptions on adjacent wireless links from the same sender are strongly correlated (called link correlation [1]) due to the existence of cross-technology interference and correlated channel fading [2]. It is experimentally verified that this characteristic has an important effect on the performance of various diversity-based network protocols. As the link correlation changes, the cost, delay, and throughput of a wireless network protocol may vary greatly. If the packet loss patterns among adjacent links are positively correlated, it is beneficial to reduce transmission cost [1]. Negative link correlation helps increase potential coding opportunities [3], but it may incur increased transmission cost. Link correlation can also assist a node in inferring the reception of packets on adjacent nodes [4] thereby reducing unnecessary retransmissions. Inspired by these features, link correlation aware protocol design is jointly considered with opportunistic routing (OR) [5]–[7], network coding (NC) [3], [8], [9], dissemination [10]–[12], flooding [13], unicast [14] and broadcast [15].

Existing link correlation aware protocols are highly dependent on link condition measurement. The most widely-used measurement method is the beacon-based protocol. Each node sends beacon messages at regular intervals and periodically shares its packet reception bitmaps to its adjacent nodes while recording the reception status of beacon messages received by its neighbors in the form of packet reception bitmaps (a "1" denoting a packet reception and a "0" denoting a packet loss). Upon receiving the bitmaps, nodes update link quality and correlation information as the basis for subsequent decisions.

For the quantification of some key metrics (e.g., expected transmission count (ETX) [16]), conventional diversity-based protocols depend mainly on link quality measurement. Apart from link quality, link correlation aware protocols rely heavily on link correlation measurement. Even if the same link quality is measured, a link may exhibit inverse link correlation with its adjacent links, along with entirely different protocol performance. Moreover, a crucial but easily overlooked detail is that deviations or perturbations in link correlation information can result in reduced protocol performance. This feature may be exploited by malicious nodes to impair protocol performance. It is noteworthy that existing malicious node detection mechanisms (whether watchdog [17], [18] or trust systems [19], [20]) only judge whether a node is malicious by monitoring its communication behaviors, and are thus incapable of tracking the attack with link correlation as a cover.

We design a link correlation spoofing attack (LCSA) in wireless networks. This is a new internal attack that exploits the vulnerability of the link correlation measurement protocol and the blind spot of existing malicious node detection mechanisms. This attack is, hidden behind the physical phenomenon of link correlation, aimed at decreasing protocol performance while escaping the detection of watchdog and trust systems. By perturbing link correlation information recorded in packet reception bitmaps but with correct link quality information, a malicious node induces its neighbors to make unreasonable decisions thereby weakening protocol performance. We analyze typical cases of OR and NC to illustrate the weakening effect of LCSAs on protocol performance clearly.

We also propose beacon-trap (BT) as a countermeasure for LCSAs, which exploits link diversity as a cover to ambush the malicious nodes. BT can be easily embedded into existing beacon-based protocols without additional control overhead

The authors gratefully acknowledge the support and financial assistance provided by the National Natural Science Foundation of China under Grant Nos. 61502230, 61501224 and 61073197, the Natural Science Foundation of Jiangsu Province under Grant No. BK20150960, the National Key R&D Program of China under Grant No. 2018YFC0808500, the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant No. 15KJB520015, the Nanjing Municipal Science and Technology Plan Project under Grant No. 201608009, and the Jiangsu Provincial Government Scholarship for Overseas Studies (*Corresponding Author: Guangwei Bai*).

978-1-5386-8088-9/19/$31.00 ©2019 IEEE

and without affecting its original functionality. With BT, nodes can set trap beacons during the periodic beacon transmissions. Thereafter, once the reception status of one trap beacon is found to be tampered with, the malicious node (the tamper) will be unmistakably identified. The localized mode of BT makes its effect not limited by the scale of a network. The effectiveness of BT against LCSAs is validated by numerical analysis in consideration of different parameter settings.

The remainder of this paper is organized as follows. The related works are presented in Section II. The implementation details of LCSA is introduced, and its attack effect is analyzed in Section III. The BT strategy to detect LCSAs is proposed in Section IV, followed by numerical results in Section V. Concluding remarks are given in Section VI.

II. Related Works

A. Link Correlation Aware Protocols

As the Internet of Things applications [21] becomes pervasive, many wireless devices share unlicensed frequency bands, leading to reception correlation at adjacent wireless links. Much research has been devoted to exploiting link correlation to optimize performance. Wang *et al.* [7] propose to choose a forwarder list consisting of positively correlated nodes to enhance OR performance. The work in [6] further considers spatial correlation among data sensed by neighboring nodes to reduce redundant relaying for OR. Zhu *et al.* [4] present the concept of collective ACKs that solves the ACK storm problem by inferring the packet reception status of correlated neighbors. Correlated flooding [22] is a link correlation aware flooding-tree protocol, which favors nodes with strong link correlation. CorLayer [15] exploits link correlation to improve the energy efficiency of reliable broadcast protocols. Correlated coding [3] balances coding opportunities and transmission cost to improve throughput by reference to link correlation. UNIV [8] is a universal NC-based OR protocol for unicast that adapts to changes in channel loss rates and link correlations. cETX [14] is a unified metric embracing both temporal and spatiotemporal correlations, which can replace ETX to facilitate data transmission. Link synergy [5] is an optimized link correlation metric, which fixes reception failures by choosing more synergic links.

The performance gain of above protocols relies on beacon-based link measurement. Packet reception bitmaps with incorrect link correlation information inevitably lead to unreasonable decisions, accompanied by performance degradation. Although a small number of improved link correlation measurement mechanisms (e.g., [2], [23]) have been proposed, the beacon-based protocol is still the most commonly used.

B. Attacks Against Network Protocols

Wireless networks are vulnerable to internal network attacks initiated by malicious nodes. Existing mainstream attack detection methods exploit communication protocols to monitor the forwarding behavior of neighboring nodes. Watchdog [18] is an internal attack detection mechanism responsible for monitoring sending behaviors of neighboring nodes. For instance, a node may be considered to be malicious if a neighboring watchdog node does not hear its forwarding. By monitoring communication behavior and estimating the trust degree of neighboring nodes, the trust system in [24] decides on whether a neighbor is benign or not by comparing its trust degree with a threshold. Reference [17] investigates resource efficient watchdog deployment issue, taking into accounts two major facts overlapping and coverage.

The watchdog mechanism is only sensitive to transmission behavior. If a malicious node implants perturbed link correlation information into the reception bitmap, it is possible to exploit the blind spot of watchdog to evade detection while degrading protocol performance. To the best of our knowledge, there have not been any similar attacks and countermeasures.

III. Link Correlation Spoofing Attack (LCSA)

In this section, we introduce the basic idea and implementation details of the LCSA, while analyzing typical cases to understand this attack more clearly.

A. Overview

The purpose of LCSAs is to degrade the performance of link correlation aware communication protocols by releasing distorted link correlation information. Specifically, a malicious node running LCSAs alters the packet reception bitmap before sharing it to neighboring beacon message senders thereby interfering with the decisions of link correlation-aware protocols and impairing protocol performance. For example, with one sender S and two receivers N_1 and N_2, let x_i denote the link from S to node N_i. Given two bitmaps "0011" and "1100" indicating the packet receptions on links x_1 and x_2 , the link correlation can be calculated by

$$C_{1,2}^{S} = \frac{\sum_{i=1}^{n} \left(b_1\left[i\right] \& b_2\left[i\right]\right)}{\sum_{i=1}^{n} b_2\left[i\right]} \tag{1}$$

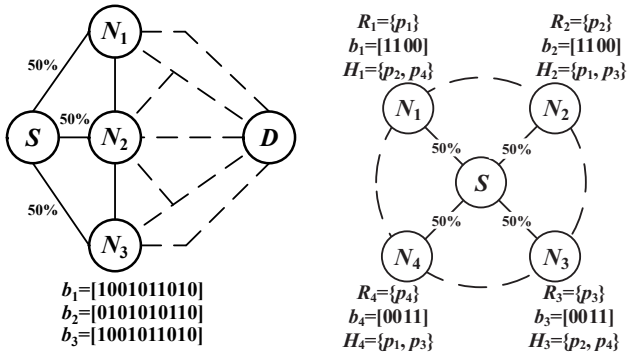
where & denotes the bitwise AND operation and $b_1\left[i\right]$ denotes the i-th bit in the bitmap of N_1. In this case, $C_{1,2}^{S}$ equals 0, which indicates that link x_1 is negative correlated with x_2. However, if N_2 generates an LCSA by maliciously changing its bitmap to "0011", then $C_{1,2}^{S}$ is equal to 1, which indicates that link x_2 pretends to be positive correlated with x_1.

There are two principles for LCSAs on malicious nodes.

- It is under the principle of providing correct link quality, i.e., while altering the reception bitmap, a malicious node does not change the number of beacon messages received (the number of "1"), which hides the fraud much better.
- The falsification of the bitmap generated by a malicious node is random, i.e., building upon the above principle, a malicious node randomly changes the fields in which the received beacon messages are located in the original reception bitmap.

B. Effect of LCSAs

We next present two typical cases (shown in Fig. 1) to illustrate how LCSAs weaken the performance of link correlation aware protocols.



(a) Opportunistic routing (b) Network coding

Fig. 1. Case examples

Case 1 (OR): Fig. 1(a) shows a simple OR topology where S is the sender and D is the destination. Let $F_{S,D}$ denote the set of candidate next-hop forwarders from S to D. Suppose that the size of a forwarder list is 2. The strength of link correlation aware OR comes from the low correlation (high diversity) of the candidates' packet receptions. Then, using (1), $\{N_1, N_2\}$ or $\{N_2, N_3\}$ will be chosen as a forwarder list with the lowest link correlation $C^S_{1,2} = C^S_{2,3} = 0.6$. The expected number of transmissions for receiving a packet from S to at least one of the two forwarders is given by

$$E\left(S, F_{S,D}\right) = \frac{1}{1 - \prod_{j=1}^{2}\left(1 - d_{x_j}\right)} \tag{2}$$

where d_{x_j} is the packet delivery ratio (link quality) of adjacent link x_j. It is computed as the ratio of the number of beacon messages received by x_j and the total number of beacon messages transmitted by S, i.e.,

$$d_{x_j} = \frac{1}{n} \cdot \sum_{i=1}^{n} b_j\left[i\right] \tag{3}$$

In Fig. 1(a), $E\left(S, F_{S,D}\right)$ with forwarder list $\{N_1, N_2\}$ or $\{N_2, N_3\}$ equals 1.43 using (2). However, if N_3 performs an LCSA, it can tamper the reception bitmap to "0110101001". After receiving such a bitmap, S mistakenly believes that link x_1 is negatively correlated with x_2, and meanwhile, it feels that selecting N_1 and N_3 as forwarders can minimize transmission cost and is, therefore, the best choice. Instead, the performance deteriorates with an increase in the resulting ETX by 0.57 (to 2), which can be verified by (2).

It is easy to imagine that if link x_2 is perfectly negatively correlated with x_1, then S will select set $\{N_1, N_2\}$ as the forwarder list, with which $E\left(S, F_{S,D}\right)$ for delivering a packet is 1. Given that the bitmap altered by N_3 is "0110100101", link correlation between links x_1 and x_3 is equal to 0 based on (1). Accordingly, the chosen forwarder list may be $\{N_1, N_2\}$ or $\{N_1, N_3\}$. If S selects set $\{N_1, N_3\}$ as the forwarder list, $E\left(S, F_{S,D}\right)$ will be doubled based on (2).

Case 2 (NC): We give a case study to validate the impact of LCSAs on NC. As shown in Fig. 1(b), S needs to transmit packets p_1, p_2, p_3 and p_4 to four receivers. Let H_i and R_i denote the set of packets owned and required at node N_i ($i \in \{1, 2, 3, 4\}$). Taking link correlation into account, the best solution for this scenario is to send the encoded packets $p_1 \oplus p_2$ and $p_3 \oplus p_4$ to reduce the number of retransmission. The ETX that S transmits a packet successfully to cover its two receivers satisfies

$$ETX = \sum_{i=1}^{2} \frac{1}{d_{x_i}} - \frac{1}{1 - d_{\overline{x_1} \cap \overline{x_2}}} \tag{4}$$

In this case, data scheduling may start with nodes N_1 and N_2, and the ETX is 4 using (4). Suppose that N_1 is a malicious node and tampers its bitmap to "0011", which means that links x_1 and x_3 are positive correlated using (1). Accordingly, if S begins with nodes N_1 and N_3 to transmit packets, it requires to encode packet p_1 and p_4 first. Next, according to (4), the ETX for successfully transmitting all the four packets reaches 6, increased by 2, i.e., one half.

Observation 1: The inaccuracy of link correlation measurement caused by LCSAs may offset the performance gain brought about by link diversity.

The untrackability of the LCSA is that the malicious node does not generate any abnormal data sending/forwarding information, making it impossible to be detected by conventional watchdog mechanisms. The confusing nature of that is that while the reception is tampered with, the link quality fed back by the malicious node is correct. Intuitively, one possible way to detect the LCSA is to allow beacon messages to be forwarded. However, even if we allow this (while ignoring the multiplication of overhead), the tracking cost is high. Thus it is necessary to investigate a new countermeasure.

IV. Beacon-Trap (BT) against LCSAs

This section presents a beacon-trap (BT) approach to capture LCSAs, consisting of its implementation details, optimal parameter settings, and theoretical analysis.

A. Overview

The principle of BT is that each node detects malicious nodes that may be hidden in neighboring nodes in a localized way, independent of node number or network size while measuring link correlation. Because BT is built on the existing beacon-based protocol that already exists for measuring link condition, our detection approach brings no additional control overhead. The main implementation process of BT is summarized as follows:

- Each node sets trap beacons in the form of waiting for the transmission time of trap beacons pre-set randomly but not always continuously when it periodically transmits beacon messages for link condition measurement.
- Each node records the transmission sequence information with a local packet bitmap, a "1" denoting a beacon transmission and a "0" denoting a trap.
- After receiving reception bitmaps, a sender can judge whether those receivers are benign or not by comparing the reception status of trap beacons between the transmission and reception bitmaps.

Take Fig. 1(a) as an example, where S needs to transmit ten beacon messages originally. Suppose that S sets a trap beacon between the second and third beacon message, during which the transmission bitmap is "11011111111". Assume that the reception bitmaps nodes N_1, N_2 and N_3 deliver to S are "10001011010", "01001010110" and "01100100101", respectively. Because $b_3[3]$ equals 1, it conflicts with the truth that S does not deliver this beacon message. Accordingly, N_3 will be identified as a malicious node performing an LCSA.

Suppose that a sender u broadcasts L beacons containing A trap beacons in each round of link measurements to an adjacent malicious node v. Based on (3), the packet delivery ratio of the link form u to v is $\frac{T}{L-A}$, where T is the number of "1" in the bitmap. The total number of possible reception bitmaps after being tampered with by v is $\binom{L}{T}$, where the number of bitmaps in the trap (i.e., the number of bitmaps in which the fields of trap beacons are maliciously modified) is

$$\begin{cases} \sum_{i=1}^{A}\binom{A}{i}\cdot\binom{L-A}{T-i}, & T>A \\ \sum_{i=1}^{T}\binom{A}{i}\cdot\binom{L-A}{T-i}, & T\le A \end{cases}$$

Once a reception bitmap released by a malicious node triggers the trap, it is bound to be captured by the node that placed the trap via BT. We define the following metric to evaluate the performance of BT.

Definition 1 (Detection Success Rate (DSR)): The DSR of u capturing v, represented by $P_u(v)$, is the ratio of the number of bitmaps v just tampers with the reception of at least one trap beacon to the total number of bitmaps, i.e.,

$$P_u(v)=\begin{cases} \frac{\sum_{i=1}^{A}\binom{A}{i}\cdot\binom{W}{T-i}}{\binom{L}{T}}, & T>A \\ \frac{\sum_{i=1}^{T}\binom{A}{i}\cdot\binom{W}{T-i}}{\binom{L}{T}}, & T\le A \end{cases} \tag{5}$$

where $W=L-A$ is the number of beacon messages actually transmitted by u (excluding the number of trap beacons A).

Following rule $p=1-\overline{p}$, we have

$$P_u(v)=1-\overline{P_u(v)}=1-\frac{\binom{W}{T}}{\binom{L}{T}}=1-\frac{W!\cdot(L-T)!}{(W-T)!\cdot L!} \tag{6}$$

Take Fig. 1(a) as an example to show how to calculate DSR, where W is equal to 10 and T equals 5. Suppose that the number of trap beacons is set to 1, i.e., L is equal to 11. When a malicious node N_3 generates an LCSA attack, the DSR calculated by (6) is $1-\frac{10!\cdot 6!}{5!\cdot 11!}\approx 0.455$.

B. Analysis

It is easy to imagine that the larger DSR is, the better effectiveness of BT will be. Hence, the optimal strategy can be expressed as maximizing DSR. Meanwhile, it is worth noting from (6) that $P_u(v)$ is only reliant on L, W, A and T.

Theorem 1: Consider a sender u, and two malicious nodes v_1 and v_2. If $d_{v_1}\ge d_{v_2}$, then $P_u(v_1)\ge P_u(v_2)$.

Proof: Assume a receiver v maintains a bitmap of length L_0, where the number of beacon messages truly transmitted is W_0. Substitute N with $d=\frac{T}{L-A}$ in (6), we get

$$P_u(v)=1-\frac{W_0!\,(L_0-d\cdot W_0)!}{L_0!\cdot(W_0-d\cdot W_0)!} \tag{7}$$

The purpose of proving $P_u(v_1)\ge P_u(v_2)$ (where $d_{v_1}\ge d_{v_2}$) is to determine the monotonicity of $P_u(v)$. Because "1" and $\frac{W_0!}{L_0!}$ are constants independent with variable d, the proof of the monotonicity of $P_u(v)$ is equivalent to proving that of the residual part (represented by $y(d)$) of (7), given by

$$\begin{aligned} y(d)&=\frac{(L_0-d\cdot W_0)!}{(W_0-d\cdot W_0)!} \\ &=(L_0-d\cdot W_0)\cdot(L_0-1-d\cdot W_0)\cdot\ldots\cdot(W_0+1-d\cdot W_0) \end{aligned} \tag{8}$$

Taking the logarithm of (8) into consideration, we have

$$\begin{aligned} \ln y(d)=&\ln(L_0-d\cdot W_0)+\ln(L_0-1-d\cdot W_0)+\ldots \\ &+\ln(W_0+1-d\cdot W_0) \end{aligned} \tag{9}$$

The derivate of (9) is expressed as

$$\begin{aligned} \frac{y'(d)}{y(d)}&=\frac{-W_0}{L_0-d\cdot W_0}+\frac{-W_0}{L_0-1-d\cdot W_0}+\ldots+\frac{-W_0}{W_0+1-d\cdot W_0} \\ &\le\frac{-W_0\cdot(L_0-W_0)}{L_0-d\cdot W_0}<0 \end{aligned} \tag{10}$$

This indicates that $P_u(v)$ increases monotonically with the increase of d (i.e., if $d_{v_1}\ge d_{v_2}$, $P_u(v_1)\ge P_u(v_2)$). ■

Remark 1: Theorem 1 shows that the higher the packet delivery ratio of a node which generates an LCSA is, the higher the probability of being captured will be.

Next, we investigate the influence of the ratio of the number of beacons indeed sent, and the total number on DSR. Let k denote the ratio of W and L, i.e., $k=\frac{W}{L}$.

Theorem 2: Consider a malicious node v and its sender list $K(v)$. If the ratio of true beacon messages and trap beacons transmitted by $u_i\in K(v)$ is approximately 2:3 (i.e., $k\approx 0.4$), then $P_{u_j}(v)\le P_{u_i}(v)$ for any $u_j\in K(v)$.

Proof: Assume the packet delivery ratio of v is d_0, and the total length of its bitmap is L_0. Substitute W with equation $k=\frac{W}{L}$ in (6), we have

$$P_u(v)=1-\frac{(k\cdot L_0)!\cdot(L_0-k\cdot d_0\cdot L_0)!}{L_0!\cdot(k\cdot L_0-k\cdot d_0\cdot L_0)!} \tag{11}$$

Similar to the proof of Theorem 1, since "1" and $\frac{1}{L_0!}$ are the given value independent with k, the maximization of $P_u(v)$ can be converted to minimize the remaining part of (11), i.e.,

$$k^*=\arg\min_{0\le k\le 1} y(k) \tag{12}$$

where k^* is the value of k when $y(k)$ is at its minimum, and

$$\begin{aligned} y(k)&=\frac{(k\cdot L_0)!\cdot(L_0-k\cdot d_0\cdot L_0)!}{[(1-d_0)\cdot k\cdot L_0]!} \\ &=(k\cdot L_0)\cdot(k\cdot L_0-1)\cdot\ldots\cdot[(1-d_0)\cdot k\cdot L_0+1] \\ &\quad\cdot(L_0-k\cdot d_0\cdot L_0)\cdot(L_0-1-k\cdot d_0\cdot L_0)\cdot\ldots\cdot 1 \end{aligned} \tag{13}$$

Taking the logarithm of both sides of (13), we have

$$\begin{aligned} \ln y(k)=&\ln(k\cdot L_0)+\ln(k\cdot L_0-1)+\ldots \\ &+\ln[(1-d_0)\cdot k\cdot L_0+1]+\ln(L_0-k\cdot d_0\cdot L_0) \\ &+\ln(L_0-1-k\cdot d_0\cdot L_0)+\ldots+\ln 1 \end{aligned} \tag{14}$$

The derivate of (14) is expressed as

$$\frac{y'(k)}{y(k)} = \frac{L_0}{k\cdot L_0} + \frac{L_0}{k\cdot L_0 - 1} + ... + \frac{(1-d_0)\cdot L_0}{(1-d_0)\cdot k\cdot L_0 + 1} + \frac{-d_0\cdot L_0}{L_0 - k\cdot d_0\cdot L_0} + \frac{-d_0\cdot L_0}{L_0 - 1 - k\cdot d_0\cdot L_0} + ... + 0 \quad (15)$$

Let $\frac{y'(k)}{y(k)}$ be 0, and we get k^* approximately equal to 0.4. ■

Remark 2: Theorem 2 shows that DSR reaches its maximum against LCSAs when a sender sets the ratio of the number of beacon messages truly transmitted (excluding trap beacons) and the length of a bitmap to 0.4 approximately in each round of link measurements.

V. Numerical Results

In this section, we evaluate the proposed attack and detection schemes in link correlated wireless networks. The results consist of two parts to study the impact of parameter settings on DSR (reflecting detection effect when the reception bitmap is received for the first time) and impact of detection duration on DSR (reflecting malicious node detection speed).

A. Impact of Network Parameters

The first set of numerical results looks at the impact of network parameters on the detection performance of BT. As shown in Fig. 2, the results on DSR are divided into multiple polylines by setting W, d, and L. By observing the impact of different network parameters, we can verify previous theoretical analysis and determine the optimal parameter settings.

Fig. 2(a) shows the impact on the effectiveness of BT exerted by the increase in packet delivery ratio when L is set to 20. The result is divided into five parts in which W is fixed to 5, 8, 12, 15, 18, respectively. With the variation of delivery ratio, DSR increases monotonically. A high delivery ratio means that the probability of a beacon-trap being lost is low, which helps to increase the DSR. As the delivery ratio reaches the upper limit, DSR reaches its peak (close to 100%).

We elaborately demonstrate the DSR of capturing nodes with different ratios of W to L in Fig. 2(b), where the packet delivery ratio is set to 0.05, 0.1, 0.2 and 0.45 separately and the ratio of W to L is set from 0.1 to 1. It can be observed that the DSR of capturing a malicious node with a high packet delivery ratio is high. We can see that the DSR does not show monotonous changes with the variation in $\frac{W}{L}$, and it reaches its maximum when $\frac{W}{L}$ equals to 0.4 for every malicious node with different packet delivery ratios. Furthermore, the higher the delivery ratio of a malicious node is, the higher the peak of its DSR is.

The influence of the ratio of the number of beacons indeed sent, and the total number on DSR is examined in Fig. 2(c), where the packet delivery ratio is set to 0.5, and the length of a bitmap L is set to 5, 10, 15, 20, and 25, respectively. The result on DSR does not change monotonously with the increase of k, and it reaches its maximum when k equals approximately 0.4. Moreover, with no traps being set (i.e., $k = 1$), DSR drops sharply to 0, which indicates the effectiveness of BT indirectly. It can also be seen that the larger L is, the higher the DSR is, and meanwhile, the better effectiveness of BT will be. A larger L, however, indicates a larger number of beacon messages to be transmitted periodically, which may lead to an inaccurate detection of link conditions due to the temporal characteristic of wireless links.

The above results indicate that by appropriately setting the length of a bitmap, a node can constrain the maximum value of DSR and the accuracy of link conditions. We can choose suitable protocol parameters according to network parameters to enhance detection efficiency.

B. Impact of Detection Duration

In Fig. 3, we analyze malicious node detection speed with BT. Considering that the time interval of each reception bitmap exchange is fixed, we use the increase in the number of exchange rounds of reception bitmaps to reflect detection duration. Besides, here we consider the detection speed at which a node can detect malicious nodes hidden in its neighboring nodes since BT works in a localized manner.

Fig. 3(a) reveals the impact of changes in the average packet delivery ratio on DSR over time, where k (equal to $\frac{W}{L}$) is fixed to 0.15. First, the increase in DSR positively correlates with the increase in delivery rate, since the increase in delivery rate increases the probability that a malicious node falls into a "trap". Second, with the increase in the number of bitmap exchange rounds, DSR increases monotonously and eventually approaches 100%. The result confirms that the speed at which a malicious node is detected is breakneck and is not subject to network size. Turning to Fig. 3(b) where d is fixed to 0.2, we aim to observe the impact of k. DSR shows a monotonous increasing trend during beacon exchange process, with the highest peak appearing when k is close to 0.4.

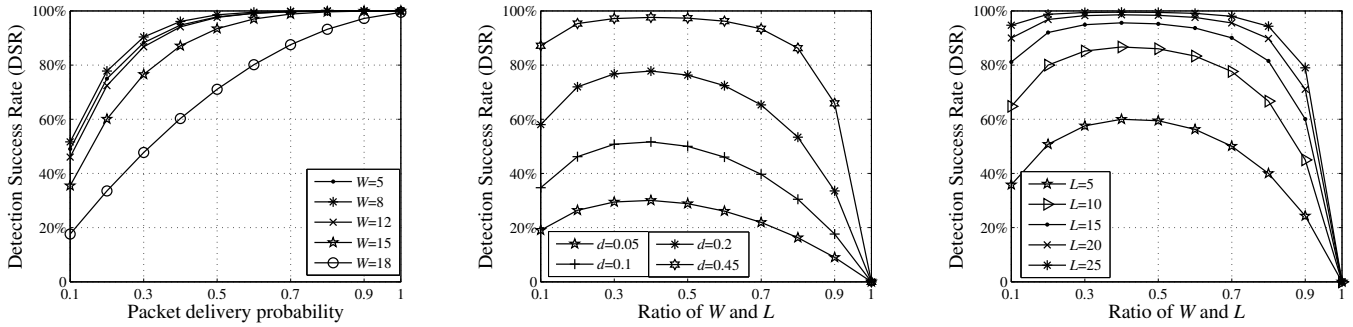
VI. Conclusion

In this paper, we present a link correlation spoofing attack (LCSA) that makes use of link correlation to camouflage to avoid being tracked by existing watchdog-like malicious node detection mechanisms. As a countermeasure, we propose a beacon-trap (BT) approach that relies on link diversity as a cover to identify malicious nodes running LCSAs. Notably, the detection capability is not limited by the network size. Our theoretical and numerical analysis demonstrates the effectiveness of BT. We also find that adjusting the ratio of the number of beacons actually transmitted and the length of a bitmap to 0.4 approximately can maximize DSR in each round of link measurements. Becuase no extra control overhead is incurred and the computational overhead is almost negligible, BT can be easily integrated into low-power network devices, replacing original beacon-based measurement protocols in those devices to cope with potential LCSAs.

References

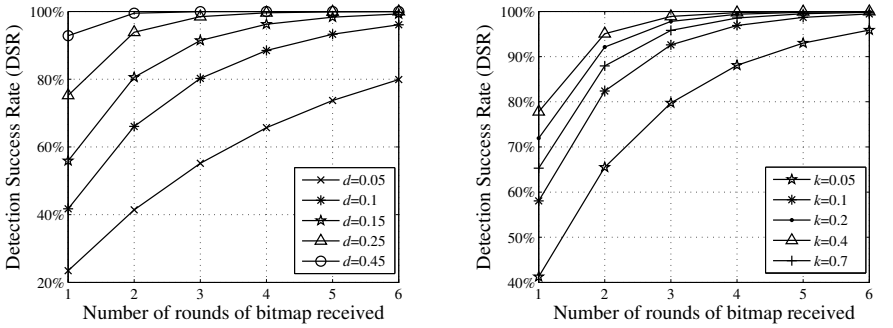
[1] K. Srinivasan, M. Jain, J. I. Choi, T. Azim, E. S. Kim, P. Levis, and B. Krishnamachari, "The k factor: inferring protocol performance using inter-link reception correlation," in *ACM MobiCom*, 2010, pp. 317–328.

[2] Z. Zhao, W. Dong, G. Guan, J. Bu, T. Gu, and C. Chen, "Modeling link correlation in low-power wireless networks," in *IEEE INFOCOM*, 2015, pp. 990–998.



(a) Impact of packet delivery ratio (b) Impact of $\frac{W}{L}$ with different packet delivery ratios (c) Impact of $\frac{W}{L}$ with different bitmap lengths

Fig. 2. Impact of network parameters



(a) Impact of different packet delivery ratios (b) Impact of k with different packet delivery ratios

Fig. 3. Impact of duration

[3] S. Wang, S. M. Kim, Z. Yin, and T. He, "Encode when necessary: Correlated network coding under unreliable wireless links," *ACM Trans. Sen. Netw.*, vol. 13, no. 1, pp. 1–22, 2017.

[4] T. Zhu, Z. Zhong, T. He, and Z. L. Zhang, "Achieving efficient flooding by utilizing link correlation in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 1, pp. 121–134, 2013.

[5] A. Kamari and M. Bag-Mohammadi, "An optimized link correlation model for opportunistic routing," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2543–2546, 2018.

[6] G. Huang, B. Zhang, and Z. Yao, "Data correlation aware opportunistic routing protocol for wireless sensor networks," in *IEEE ICC*, 2017, pp. 1–6.

[7] S. Wang, A. Basalamah, M. K. Song, S. Guo, Y. Tobe, and T. He, "Link-correlation-aware opportunistic routing in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 47–56, 2015.

[8] A. Khreishah, I. Khalil, and J. Wu, "Universal network coding-based opportunistic routing for unicast," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1765–1774, 2015.

[9] S. I. Alam, S. Sultana, Y. C. Hu, and S. Fahmy, "Syren: Synergistic link correlation-aware and network coding-based dissemination in wireless sensor networks," in *IEEE MASCOTS*, 2013, pp. 485–494.

[10] Z. Zhao, J. Bu, W. Dong, T. Gu, and X. Xu, "Coco+: Exploiting correlated core for energy efficient dissemination in wireless sensor networks," *Ad Hoc Netw.*, vol. 37, pp. 404–417, 2016.

[11] W. Dong, Y. Liu, Z. Zhao, X. Liu, C. Chen, and J. Bu, "Link quality aware code dissemination in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1776–1786, 2014.

[12] Z. Zhao, W. Dong, J. Bu, Y. Gu, and C. Chen, "Link-correlation-aware data dissemination in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 9, pp. 5747–5757, 2015.

[13] X. Shen, Y. Chen, Y. Zhang, J. Zhang, Q. Ge, G. Dai, and T. He, "Oppcode: Correlated opportunistic coding for energy-efficient flooding in wireless sensor networks," *IEEE Trans Ind. Informat.*, vol. 11, no. 6, pp. 1631–1642, 2015.

[14] S. M. Kim, S. Wang, and T. He, "cetx: Incorporating spatiotemporal correlation for better wireless networking," in *ACM SenSys*, 2015, pp. 323–336.

[15] S. Wang, M. K. Song, Y. Liu, G. Tan, and T. He, "Corlayer: a transparent link correlation layer for energy efficient broadcast," *IEEE/ACM Trans. Netw.*, vol. 23, no. 6, pp. 1970–1983, 2015.

[16] D. S. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wirel. Netw.*, vol. 11, no. 4, pp. 419–434, 2005.

[17] M. M. Hasan and H. T. Mouftah, "Optimization of watchdog selection in wireless sensor networks," *IEEE Wirel. Commun. Lett.*, vol. 6, no. 1, pp. 94–97, 2017.

[18] E. Hernandez-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Cocowa: A collaborative contact-based watchdog for detecting selfish nodes," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1162–1175, 2015.

[19] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for wsns," *IEEE Trans. Inf. Forensics Security.*, vol. 10, no. 3, pp. 613–625, 2015.

[20] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, 2015.

[21] Q. Ye and W. Zhuang, "Distributed and adaptive medium access control for internet-of-things-enabled mobile networks," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 446–460, 2017.

[22] S. Guo, S. M. Kim, T. Zhu, Y. Gu, and T. He, "Correlated flooding in low-duty-cycle wireless sensor networks," in *IEEE INCP*, 2011, pp. 383–392.

[23] Z. Zhao, X. Xu, W. Dong, and J. Bu, "An accurate link correlation estimator for improving wireless protocol performance," *Sensors*, vol. 15, no. 2, pp. 4273–4290, 2015.

[24] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," *Comput. Commun.*, vol. 33, no. 9, pp. 1086–1093, 2010.