Alibi: A framework for identifying insider-based jamming attacks in multi-channel wireless networks

[Extended Abstract]

Hoang Nguyen
hnguyen5@uiuc.edu

Thadpong Pongthawornkamol
tpongth2@illinois.edu

Klara Nahrstedt
klara@illinois.edu

ABSTRACT

We consider the problem of identifying the insider-based attacks in the form of jammers in multi-channel wireless networks, where jammers have the inside knowledge of frequency hopping patterns and any protocols used in the wireless network. While this type of attackers is dangerous, most of current state-of-the-art jamming detection solutions cannot cope with them. In this work, we propose a novel technique, called "**alibi**", to identify the insider-based jammers in multi-channel wireless networks. Alibi is a form of defense whereby a defendant attempts to prove that he or she was elsewhere when the crime in question was committed. Starting from such a simple concept, we develop an alibi framework to cope with insider-based jamming attackers in various situations including lossy channels, single jammer and multiple jammers. We evaluate the framework according to several properties such as accuracy, detection time & network performance in ns2 simulation and analysis. The overall results of these protocols show a promising research direction to deal with insider-based jamming attacks.[1]

1. INTRODUCTION

Radio jamming is an inherent problem of wireless networks due to its open and shared nature of the medium. In an jamming attack, an attacker injects a high level of noise into the wireless system which significantly reduces the signal to noise and interference ratio (SINR) and probability of successful message receptions. While there are various ways to carry out jamming attacks, we consider a so-called *insider-based jamming attack* as follows. In an insider-based jamming attack, there are several nodes getting compromised either before the deployment or during the operation of the network. These compromised nodes become means to jam the network. The dangers of this type of attacks are two-fold. First, the attackers have any shared knowledge supposed to remain secret within the network such as shared keys, shared hopping pattern and/or any protocols used by the network. Second, the attackers can be very stealthy if they want to stay undetected as long as possible to do further damage to the network. The stealthy nature of the attack also helps the attackers to conserve the energy if the devices are powered by batteries.

Most of the work in the jamming defense literature can only deal with outsider-based jamming attacks [2, 3, 4, 5, 6]. By "outsider", we mean the attackers with zero knowledge of any shared secrets among nodes in the network. One of the most effective ways to prevent such an outsider jammer is spread spectrum technique. By hopping the carrier frequency (frequency-hopping spread spectrum - FHSS) or spreading its signal in time (direct-sequence spread spectrum - DSSS), the network can force the jammer to spend several-fold more power than if spread spectrum were not used[7]. However, spread spectrum does not work if the attacker knows the hopping-pattern of the FHSS or the pseudo-noise chip sequence of DSSS. An insider-based jammer can easily obtain the shared hopping pattern of the network and jam very effectively. Thus, dealing with insider-based attackers is far more challenging than the outsider-based ones.

We focus on the problem of *identifying* the insider-based jammers. Note that there is a difference between detection and identification. Detection is a weaker concept than identification. Detection only means that a jammer exists. Identification means that a node X is the jammer. We propose a novel technique, called "**alibi**", to identify insider-based jammers in multi-channel wireless networks. By definition, *"alibi is a form of defense whereby a defendant attempts to prove that he or she was elsewhere when the crime in question was committed"*. In the context of jamming attacks, *honest nodes try to obtain alibis showing that they were doing legitimate actions observed by some witnesses while the jamming action took place.* From this core concept of alibi, we develop a framework, called **alibi framework**, including a set of randomized algorithms and protocols to identify insider-based jammers. The key principle in building the alibi framework is that there has to be a significant difference in the way of obtaining alibis between honest nodes and attackers. For example, alibi can be defined in the way that only honest nodes can obtain alibis while attackers cannot obtain any alibis. In this way, when all honest nodes obtain at least one alibi, attackers are identified.

We have identified numerous challenges in applying the alibi concept to our problem. First, wireless networks are *inherently lossy/unreliable* and there is no clear distinction between a "normal-corrupted" packet (i.e. a packet corrupted by an unintentional collision) and a jammed packet (i.e. a packet corrupted by an intentional jamming action). Thus, we may get "false" alibis that are falsely generated from misidentified lossy event. Second, alibi is susceptible to *slander attacks.* In a slander attack, if the behaviors of honest nodes are *completely known* by the attackers, the attackers can *deterministically* avoid committing jamming actions whenever victim honest nodes can potentially obtain alibis. By doing this strategy, the victim nodes will never be able to obtain any alibis and thus become as misidentified as attackers. Third, there might be multiple attackers in the network.

[1]This material is based upon work supported by the National Science Foundation under Grant CNS-0524695 and Vietnam Education Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of those agencies.

A jam event caused by one attacker can generate alibi for another attacker. Last but not least, alibi framework has to be able to cope with all these challenges without much performance degradation of the network.

We have addressed the case of single jammer, lossy channel condition and multiple non-colluding attackers [10]. We are working on the case of multiple colluding attackers [9]. However, due to the space limitation, we only present the case of lossy channel and multiple non-colluding attackers.

2. SYSTEM MODEL

2.1 Network Model

We consider a multi-channel wireless network where some nodes in the network are insider-based jammers. We assume that these jammers can affect at least several nodes (if not all) of the considered wireless network. Specifically, the network has n nodes $N_1..N_n$ in which a node can send/receive to several other nodes. Nodes in the network have a set of C orthogonal channels $\Gamma = \{\gamma_1, ...\gamma_C\}$ that they can switch to. These channels may not be necessarily contingent in frequency. Each node is equipped with a single transceiver. That means, a node cannot send and receive simultaneously. There will be also non-negligible transmit-to-receive and receive-to-transmit turn-around time. The channel switching delay of a node is also assumed to be non-negligible. Nodes in the network use a multi-channel MAC protocol such as Slotted Seeded Channel Hopping (SSCH) [1] or McMAC [11] because these MAC protocols improve network capacity and eliminate the problem of single control channel bottleneck which is a sweet spot for the jammer to target on. We only consider centralized detection model. In the centralized detection model, we assume there is a trusted entity G where nodes can report to. This entity can sit on the wireless network such as the base station or can be in the Internet. We also assume that every node knows the public key k_G of G. This will make sure nodes can have a secure communication to G when necessary.

3. ALIBI'S FRAMEWORK

3.1 Alibi

Alibi is a form of defense whereby a defendant attempts to prove that he or she was elsewhere when the crime in question was committed. The alibi framework is built up from this core concept. Our alibi definition is as follows.

DEFINITION 1 (ALIBI & DEFENDANT). *An alibi for a defendant is a proof including time and channel information which shows that the defendant was doing legitimate actions at the time the jamming action was committed. A legitimate action is either sending or receiving a packet.*

DEFINITION 2 (PROOF & WITNESS). *A witness is a node who shows a proof of a defendant doing an action at a specific time.*

In our alibi framework, a defendant cannot claim an alibi by himself. Rather, witnesses generate alibis for defendants from collected proofs.

DEFINITION 3 (RECEIVING-BASED ALIBI (R-ALIBI)). *A receiving-based alibi for a node (referred to as* R-defendant*) shows that the defendant was receiving a jammed packet, by showing a (hashed) packet content that matches with the (hashed) packet content received by other witnesses (referred to as* R-witnesses*).*

This definition exploits the fact that a node cannot both send and receive a packet simultaneously. In the receiving-based alibis, an R-defendant of a jamming event is also an R-witness of other R-defendants of the same event. In other words, a group of nodes that can show the same hash of a jammed packet content in the same time slot will all receive R-alibis.

We also have the definition of sender-based alibis (S-alibis). However, we found that S-alibis are very susceptible to slander attacks [8]. Thus we only consider R-alibis only.

3.2 The principle in using alibis

The key principle in using alibis to identify attackers is that there has to be significant difference of alibis obtained by good nodes and attackers. The difference can be deterministic such as "only good nodes can obtain alibi while attackers cannot" or statistical such as "a good node statically obtains higher number of alibis than an attacker". With these differences, as time goes on, the attackers will be eventually identified. If attackers can manage to remove the differences, the alibi framework will fail to differentiate the good nodes and the attackers.

3.3 A basic alibi-based protocol

When an honest node is idle in any time slots (i.e. no sending or receiving), it switches to a uniformly random channel in Γ with probability p_w to become an R-witness (also R-defendant). For a node, increasing p_w will increase the probability of being R-witness and potentially increase the probability of getting alibis but also decrease its network performance. For example, if a node has always a packet to send, $p_w = 0.2$ means it will lose 20% of its either sending or receiving. Thus, p_w can be used as a parameter to control the trade-off between the probability of getting alibis and the degradation of the network performance.

When a node N_i becomes a R-witness in a time slot t on channel c, it will receive the whole packet content p regardless of whether the packet is decodable or not. It will get the hashed content of the received packet by using any good hash function H (e.g. CRC, SHA1 or MD5) and create a proof m in the following form:

$$m = (N_i, t, c, < H(p) >_{k_G}, H(N_i, t, c, H(p))).$$

3.4 Desired Properties

- **Detection time**: this property is concerned about the time to detect the attackers.
- **Accuracy**: this property is concerned about the false alarm and miss detection.
- **Availability/Network performance**: this property defines fraction of time the channels is available for communication.

4. DEALING WITH A SINGLE ATTACKER UNDER LOSSY CHANNELS

There are two main issues for alibi framework when channels become lossy. First, a lossy event may be falsely treated as a jamming event. Second, due to such mistreatment of loss events, an jammer may accidentally get "false alibis" if he follows the alibi protocol. Because we assume that there is no difference between a lossy event and a jamming event, we accept the fact that there might be "false alibis". In other words, the jammer can obtain "false' alibis but so can honest nodes. Thus, *the fundamental difference between an honest node and the jammer is that honest nodes can obtain both "true alibis", i.e. alibis from the jamming event, and the "false alibis" while the jammer can only obtain the "false alibis".* By exploiting this fact, it appears that the rate at which an honest node obtains both types of alibis might be higher than the rate at which the jammer obtains false alibis. Once we ensure that any honest node can obtain alibis faster than the attacker, we can use any statistical detection techniques to differentiate the honest nodes and the

attacker. By analysis, we have shown that if the system wants to detect an attacker with the minimal jamming rate p_j^{min}, p_w has to satisfy $p_w > p_l \frac{(1-p_j^{min})}{p_l+p_j^{min}}$.

5. DEALING WITH NON-COLLUDING JAMMERS

Let us assume there K jammers in the system ($1 < K < C$). We assume these jammers do not collude by any means. We also assume that all jammers have the jamming probability of p_j in each time slot. We assume a jammer picks a channel to jam uniformly in Γ. Furthermore, as similar to the case of lossy channel, we assume these K jammers will never have overlapping jamming pattern. We do not consider overlapping jamming slots because they waste the attackers' jamming efforts and will not create any extra alibis for good nodes. Thus, in every time slot K random but distinct channels are jammed by K non-colluding jammers.

By analysis, we have shown that if the system wants to detect K attackers with the minimal jamming rate p_j^{min}, p_w has to satisfy $p_w > \frac{(K-1)(1-p_j^{min})}{K}$.

6. SIMULATION RESULTS

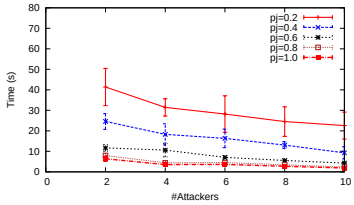

Figure 1: Average detection time

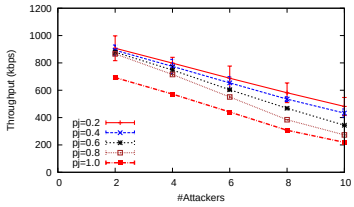

Figure 2: Average throughput

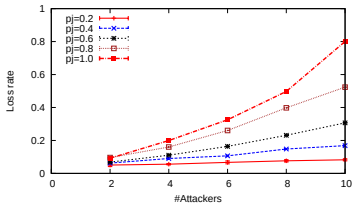

Figure 3: Average loss rate

We evaluate the proposed protocol in ns2. We implement a simplified version of SSCH. SSCH is built on top of 802.11b physical layer. CSMA/CA is used to resolve the contention of nodes on the same channel. RTS/CTS mode is disabled. The bandwidth is 11Mbps. Nodes are placed so that they can communicate with each other in one hop. Each node has at least one constant-bit rate (CBR) flow to another node. Each CBR transmits packets of 512 bytes for every 10ms. This will guarantee that nodes always have packets to send to fully utilize the network. The network uses 11 channels to communicate[2]. We vary the percentage of attackers and jamming probability of the jammer in the network. Each scenario is repeated 10 times to get the average and deviation. As shown in Figure 1, when the number of attackers or the jamming rate increases, the attackers get caught faster. This matches with the principle of alibi framework: more jammed packets will lead to more alibis for honest nodes and thus faster detection time. Figure 2 and 3 show the throughput and loss rate of the network under different number of jammers. In our simulation, a false alarm is declared when an honest is falsely accused as an attacker and a miss detection is declared when not all attackers are identified after $T = 2000$. In all simulation scenarios, we had zero false alarms and extremely low miss detection rate (less than 0.01%). Therefore, we do not show them here. This shows an advantage of sequential hypothesis testing when false alarm and detection probability are the main parameters.

[2]SSCH requires the number of channels to be a prime number.

7. CONCLUSION & FUTURE WORK

The problem of identifying insider-based jammers in multi-channel wireless networks is a challenging problem and has not been addressed in the literature. We have shown the alibi framework to cope with this type of attackers. We also have shown detailed study of properties of alibi framework including accuracy, detection time and network performance, by both simulation and analysis.

There are still several challenging problems for alibi framework. First, we need to have a distributed detection scheme to make alibi framework scalable. This includes protocols and algorithms for exchanging proofs and alibis among honest nodes. Second, we also need to address multi-hop multi-channel wireless networks. In a multi-hop wireless network, attackers may lie in different areas of the network and may form a different jam strategy to confuse the alibi detector. Thus, we needs to have handle the attackers differently.

8. REFERENCES

[1] P. Bahl and R. Chandra. SSCH: Slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks. In *ACM MobiCom*, 2004.

[2] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In *MobiHoc*, 2006.

[3] J. T. Chiang and Y.-C. Hu. Dynamic jamming mitigation for wireless broadcast networks. In *INFOCOM*, 2008.

[4] L. C. B. III, W. L. Bahn, , and M. D. Collins. Jam-resistant communication without shared secrets through the use of concurrent codes. Technical report, U.S. Air Force Academy, 2007.

[5] P. Kyasanur and N. H. Vaidya. Detection and handling of MAC layer misbehavior in wireless networks. In *DSN*, 2003.

[6] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein. Using channel hopping to increase 802.11 resilience to jamming attacks. In *INFOCOM Minisymposium*, 2007.

[7] R. Negi and A. Perrig. Jamming analysis of mac protocols. Technical report, Carnegie Mellon Technical Memo, 2003.

[8] H. Nguyen, T. Pongthawornkamol, and K. Nahrstedt. Alibi: A novel approach for detecting insider-based jamming attacks in wireless networks. Technical report, UIUC, 2008.

[9] H. Nguyen, T. Pongthawornkamol, and K. Nahstedt. Alibi: A framework for identifying insider-based jamming attacks in multi-channel wireless networks. In *INFOCOM (in submission)*, 2009.

[10] H. Nguyen, T. Pongthawornkamol, and K. Nahstedt. Identifying insider-based jammers in single-hop wireless networks. In *MILCOM*, 2009.

[11] H.-S. W. So and J. Walrand. McMAC: A multi-channel MAC proposal for ad-hoc wireless networks. Technical report, UCB Tech. Report, 2005.