MeshJam: Intelligent Jamming Attack and Defense in IEEE 802.11s Wireless Mesh Networks

Yu Seung Kim, Bruce DeBruhl, and Patrick Tague
Carnegie Mellon University
Email: {yuseungk, debruhl, tague}@cmu.edu

***Abstract*—Wireless mesh networks represent an emerging network architecture which has been actively studied and standardized for the last several years. Because of their flexible network architecture, wireless mesh networks can provide alternative paths even when wireless links are broken by node failures or routing attacks. Among a variety of mesh network protocols, we focus on the recently ratified IEEE 802.11s WLAN mesh standard. With analysis of the path selection scheme in 802.11s, we show the effect of conventional jamming on 802.11s-based wireless mesh networks via simulation. We then introduce mesh jamming, which can more efficiently attack the mesh path selection process by exploiting cross-layer knowledge and more harmfully influence on the path discovery performance compared to conventional jamming. We propose a proof-of-concept defense, bi-directional path discovery to mitigate the devastating effect of mesh jamming.**

I. Introduction

Over the past few years, due to high demand, research and industry communities have actively studied various types of wireless mesh networks. Recently, the IEEE 802.11s mesh standard [1] was ratified as an amendment to the popular Wi-Fi networking standard. Owing to their flexibility, wireless mesh networks are becoming essential parts of the next-generation network architecture. The nodes in wireless mesh networks can communicate with other nodes which are not in their wireless coverage with the help of intermediate forwarding nodes. Since they are free from the direct connection limitation to the central point of the network, it is easy to extend the network coverage and to balance the network load in a distributed manner. Besides, wireless mesh networks do not need to have a strict flat structure from the traditional ad hoc networks, which has made their real deployment sluggish. The nodes in mesh networks can have vertically hierarchical mapping structure while having horizontally equal peer nodes.

One of the advantages of wireless mesh networks is the high service availability supported by multiple routes (*i.e. path redundancy*) which can reduce risks from single point of failure. Most mesh path selection mechanisms such as Ad hoc On-Demand Distance Vector Multipath (AODVM) [2], provide such path redundancy. Path redundancy is a classical research topic as a part of network fault tolerance. However, most of these studies only focus on the failure of a small number of nodes or links. For example, in Rope Ladder Routing (RLR) [3], Lessmann *et al.* propose a routing mechanism to form a rope-ladder structure which can provide ideal backup scheme. However, an attacker can use jamming, an attack emitting intentional noise to interrupt the legitimate communication, disrupting the communication of a large number of nodes in wireless mesh networks. The conventional path backup approach cannot therefore effectively recover from the multiple jammed links.

Although jamming is originally perceived as a physical-layer attack, an attacker can use cross-layer information to more effectively interfere with network flows. For example, Tague *et al.* define *flow-jamming* which optimizes the jamming transmission power and the workload allocation [4]. This new type of jamming is therefore considered to be a network-layer threat that severely degrades the routing performance in wireless mesh networks. Recent studies have proposed methods which address the jamming problem in the wireless ad hoc network domain. Wood *et al.* provide a mechanism to map the jamming area, which can help the packets to evade the damaged region [5]. However, it is questionable if it is a practical solution due to the long time to map the jammed region and the concerns about congestion around the jammed region for delivering jamming information. Mustafa *et al.* propose a path selection method based on the jamming attack history vector (AHV) [6], in which a node collects all the attack history of each link in the network during a given period and calculates the optimal path by a greedy algorithm to avoid the computational overhead in a prohibitively large search space. This centralized approach, however, still requires high communication cost for delivery of AHVs and high optimization cost. Moreover, it is impossible to collect all the necessary information of all links in the network under jamming. Kim *et al.* propose a detouring method using multiple paths (DMP) against jamming [7]. DMP is an algorithm to divide a network into multiple grid zones and to find optimal detouring paths from the zone of the source node to the zone of the destination node by avoiding the intermediate jamming zones. This mechanism, however, requires that every node knows the geographical locations of itself and its neighbors, which is not always possible. It also suffers from the same weaknesses as jammed area mapping [5].

In this work, we show that an attacker can severely degrade path selection in wireless mesh networks with only a small amount of information about the mesh protocols. Of many types of practical wireless mesh networks, we choose the IEEE 802.11s [1] based WLAN mesh. The *hybrid wireless mesh protocol (HWMP)* in this standard consists of an on-demand routing part which is fundamentally similar to Ad hoc On-

Demand Distance Vector (AODV) protocol [8] and a tree-based proactive routing part. In this paper, we propose *mesh jamming* and demonstrate that it can more severely disturb the operation of HWMP with greater efficiency than conventional jamming. We also propose a proof-of-concept defense mechanism which can complement HWMP and mitigate the effects of mesh jamming.

The rest of this paper is organized as follows. In Section II, we explain the system model and our IEEE 802.11s wireless mesh network simulator. We introduce the concept of mesh jamming in Section III. We also provide the simulation results showing the effect of each type of jamming on the wireless mesh networks and analyze the vulnerability in the IEEE 802.11s protocol. We then propose defense mechanisms against mesh jamming and demonstrate their effectiveness in Section IV. We conclude the paper in Section V.

II. System Model and Assumptions

In this section, we describe our system model and the assumptions made in our simulator used to measure the jamming effect on wireless mesh networks.

A. System Model

We assume a wireless mesh network consists of widely deployed Wi-Fi nodes. The network follows the IEEE 802.11s WLAN mesh network standard. The network purely consists of mesh clients without any root node, which is similar to the non-hierarchical ad hoc network configuration. Mesh clients form one *mesh basic service set (MBSS)* without having any extension to another MBSS by mesh gate or to different type of LAN by mesh portal. According to the IEEE 802.11s standard, we define each mesh node as a **nomadic** type of node, not fully mobile. A **single channel** is used for all mesh nodes, so it is not possible for the mesh nodes to spectrally evade jamming by changing frequency.

In the MAC layer, each mesh node operates on the contention-based channel access scheme. We do not consider the contention-free MCCA (MCF controlled channel access), which is optional in the standard. Each mesh node uses a **rate adaptation** mechanism which changes the data rate depending on the signal-to-interference-noise ratio (SINR), i.e. the data rate increases as the SINR value becomes high[1]. Thus, the data rates of a wireless link in both directions are **asymmetric** to each other depending on the surrounding channel condition.

IEEE 802.11s defines HWMP, which is a combination of an on-demand path selection with a tree-based proactive path selection. Since the path created by the proactive path selection is inefficient, temporal, and available only when a root node exists in a MBSS, we consider only the **on-demand path selection** of HWMP. The on-demand path selection operates similar to the AODV [8] protocol in using *path request (PREQ)* and *path response (PREP)* for path discovery.

The attacker can deploy **multiple jammers** over the target mesh network. Due to concerns about the detectability and the resource constraints, each jammer transmits noise with the **limited power** and the **randomized on/off duty cycle**. In order to increase attacking efficiency, the jammer uses a **sensing capability** which can interpret the header of mesh frames. This can be implemented by a separate radio listening to the channel and informing the jamming radio whenever it detects the transmission of mesh frames of interest. It is also possible by one radio which can simultaneously process the sensing and jamming operations due to the recent advance in interference cancellation technology [11].

[1]We assume each node can estimate the SINR. Various approaches have been proposed in recent literature [9] [10].

B. Simulation Assumptions and Setup

Even though there is already an implementation [12] of the IEEE 802.11s protocol in the Linux platform, we decide to build our own simulator for ease of testing with a large number of nodes. We implement the on-demand path selection of HWMP in IEEE 802.11s with the Python language. The simulation follows the *line-of-sight (LOS)* signal propagation model [13] to calculate received signal strength in each node. We set all the antenna gains to 1, and set the path-loss exponent to 2.4. At the center frequency of 2.4 GHz ISM band, the wavelength is calculated as 0.1249m. Note that our results do not depend on this LOS model, so similar results are expected with NLOS or fading models. The clear channel assessment (CCA) threshold in each node is set to -82 dBm, and the noise floor is set to -95 dBm. In accordance with the standard IEEE 802.11g parameters [1], each node also changes its rate from BPSK 1/2 to 64-QAM 3/4 depending on the $SINR$ observed from previous frame transmission. Note that this rate adaptation is used only when a node transmits unicast frames. Broadcast frames are always sent at the base rate (6 Mbps in this case) because there should be an agreement for receiving among the nodes using different rates. For unicast frames, a maximum retransmissions will follow if the transmitting node cannot receive the ACK frame from the receiving node. Broadcast frames are not followed by ACK frames, so no retransmission occurs.

Each node is allowed to transmit with power ranging from 0 dBm to 20 dBm, and we randomly assign transmission power to each node to simply emulate the irregular signal attenuation by surrounding obstruction. Based on the given configuration, the maximum reachable distance of transmitting frames from each node is calculated as 35 meters at 0 dBm and 244 meters at 20 dBm. A pair of nodes establish a wireless link between them only if both of their frames are reachable to each other. We assume that jammers also transmit within the same power range.

III. Mesh Jamming in IEEE 802.11s Networks

Based on the aforementioned system model in Section II, we analyze the jamming effect on wireless mesh networks in simulation. We show the effect of conventional jamming and introduce *mesh jamming* which exploits the cross-layer knowledge by sensing the mesh frame and selectively attacks a certain type of mesh frame. We also provide simulation results

to compare the effects on the mesh network with each type of jamming.

A. Mesh Jamming

The conventional jammer does not have any knowledge about the frame over the wireless channel. To evade jamming detection and improve efficiency, the attacker may try to randomize its duty cycle instead of constantly transmitting jamming signal over the wireless channel.

If the jammer can sense the channel and determine the frame type (*i.e.*, reactive jamming [14] [15] [16]), it is possible to launch an attack which is more devastating to the target network and more efficient for the jammer itself. As a cross-layer extension of reactive jamming, we define *mesh jamming*, which determines the type of mesh frames and selectively interrupts the transmission of certain type of mesh frames. For example, the mesh jammer can determine the type of mesh frame by reading the type field, sub-type field, and element ID field. The mesh jammer listens to the channel and switches to the receiving phase whenever it detects any frame transmission. If the transmitting frame is found to be the target mesh frame after reading the header part of frame, the jammer quickly turns on the jamming radio to jam the remaining part of the frame. Otherwise, it returns to the listening phase.

We focus on the three major types of mesh frames used in the on-demand path selection of HWMP: PREQ, PREP, and *path error (PERR)*. The PERR frame is generated when any node senses that the current link status has been changed. By jamming the PERR frames, the attacker may delay the new path request process in each node. In this study, we consider only the mesh frames which directly affect the path discovery process. Thus, we define the three types of mesh jamming.

- PREQ jamming: jams only the PREQ frames
- PREP jamming: jams only the PREP frames
- PREQP jamming: jams both the PREQ and PREP frames

We assume that it is difficult for the attacker to selectively jam the ACK frame, since the length of ACK frame is relatively short and it is a unicast frame which can be sent at a high rate, thus being transmitted for a short time period. For the analysis of worst case from the perspective of target network, we assume that the mesh jammer can always jam the target frames.

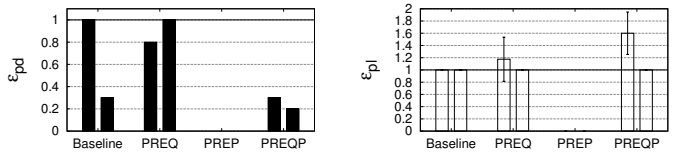
B. Simulation Results

In order to compare the effects of each type of jamming, we conduct various experiments in our simulation. For the baseline performance, we use the constant jammer as a conventional jammer. Note that the impact of constant jammer is equal to reactive jammer since both jammers jam all types of frames. With the simulator described in Section II-B, we randomly generate a mesh network which consists of 50 mesh nodes and two jammers. The use of more jammers will be easily detected and the mesh network cannot provide any path redundancy, and thus we do not consider this case. We choose two different paths crossing the jammed region. The maximum retransmission is set to 7, which is common in many implementations.

For the quantitative comparison of jamming effect, we use the probability pd of path discovery and the hop length l of discovered path. Thus, we define the following metrics.

- $\epsilon_{pd} = pd_{jam}$
- $\epsilon_{pl} = l_{jam}/l_{nojam}$

The subscript represents whether the jamming is on or off for each measurement.

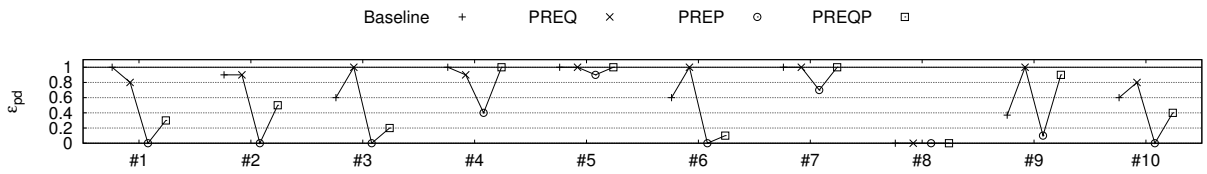


(a) Path discovery probability expansion (b) Path length expansion

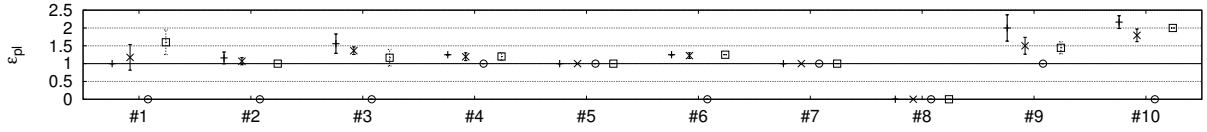
Fig. 1: Various jamming effects on mesh network (600x600)

We repeat the simulation 10 times for each jamming attack type and depict the averages and variations of each metric for two paths in Fig. 1. The average m is shown as the height of each box and the error bar is defined as $(m - \sigma, m + \sigma)$, where σ is the standard deviation over the 10 trials. As shown in Fig. 1(a), all of four types of jammer interferes with path discovery. The baseline jammer and PREQ jammer show relatively less devastating performance in terms of path discovery, but both of them to some extent increase path length for the discovered paths. Different from the expectation that the baseline jammer will be more harmful than the others since it jams more frames, it is interesting that the PREP jammer completely prevents the discovery of two paths for 10 trials by only jamming PREP frames. This means that the PREP jammer can be more devastating than the baseline jammer even with less energy spending.

To verify that this trend generally holds in other cases, we extend the simulation in 10 different configurations for each of two different size of areas (300x300 and 600x 600 square meters, respectively). In Fig. 2, we plot the measurements of one path (for the purpose of distinguishable presentation) in 10 different configurations over 600x600 square meters area. In the configuration #5 and #7, all jammers cannot severely degrade the path discovery probability because there are many back-up routes to detour the jammed region. On the other hand, the configuration #8 is far less resilient to jamming since the jammers are placed in critical points for path discovery. Overall, the PREP jammer still has the most harmful impact on the mesh network. Except for the configuration #9, the PREQP jammer shows the second best performance. The baseline jammer shows slightly better performance than the PREQ jammer except for the configuration #1 and #4. We omit the results over 300x300 square meters area (dense configuration) because it also shows similar trends.



(a) Path discovery probability expansion



(b) Path length expansion

Fig. 2: Jamming effects on 10 different configurations (600x600)

C. Analysis

The baseline jammer blocks the transmission of all types of frames. Compared to the PREQ jammer, the baseline jammer is therefore more influential to the path discovery as shown in most cases of Fig. 2(a). However, the PREP jammer and the PREQP jammer are otherwise superior to the baseline jammer. The PREQ frames are easily broadcast via redundant paths even part of links in the path is jammed. If the redundant paths are distant from the jammed region, the frame delivery ratio (FDR) over path will be even higher. This also explains why the PREP jammer disrupts path discovery most effectively. Once the unicast PREP frames are jammed in the vicinity of jammer, it is not easy to recover even with retransmission. The PREQP jammer makes the HWMP find the path detouring jammed region in the course of PREQ propagation, and thus the following PREP can be easily delivered over the less likely jammed path.

On the other hand, the baseline jammer is supposed to be more interfering than the PREQ jammer on the PREP delivery. If, however, the path found during the PREQ propagation detours the jammed region, the baseline jammer cannot influence much on the PREP delivery. This happened in the configuration #1 and #4 of our experiment, so the performance inversion between the baseline jammer and the PREQ jammer is observed although statistically a small difference.

Last but not least, the fact that PREQ is always sent at low rate contributes the inferior performance of PREQ jammer. The FDR of broadcast PREQ in a link is higher than unicast PREP due to the robust modulation technique. This also increases the FDR of PREQ compared to PREP under the same amount of jamming power.

As observed in our simulation, the mesh jammers are not only more energy efficient by selectively jamming, but also more devastating than conventional jammer. Moreover, these jamming techniques do not affect the airtime link metric which is used for path selection in HWMP since it only jams a small number of frames, thus making even harder to detect the attack and to provide alternative paths.

IV. Defenses against Mesh Jamming

From the simulation study, we found that the on-demand path selection can sometimes provide much better path than the original one by only switching the source node and the destination node of a path. This is because the mesh jammers have the directivity for attacking paths. Inspired by this observation, we can think of the bi-directional path discovery, which tries to discover the path both from source to destination and vice versa, and then selects the better path between the found ones depending on the metric of interest.

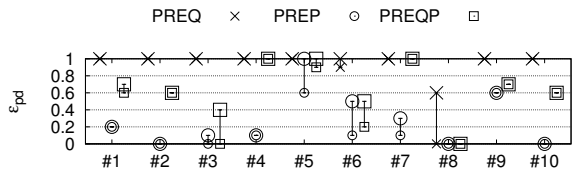
We simulate the bi-directional path discovery, which selects shorter length path if two paths are discovered, so as to see its performance gain in jamming resiliency. We define another metric to quantify the performance of defenses by extending the jamming effect metrics.

$$\delta_{pl}^{[bdp]} = \epsilon_{pl}^{[bdp]} / \epsilon_{pl}^{[jam]}, \tag{1}$$

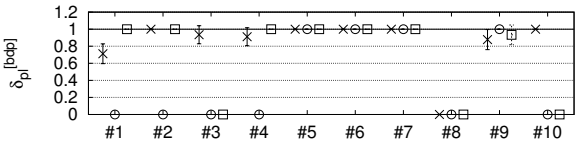
where $\epsilon_{pl}^{[bdp]}$ is the expansion of path length when the defense method is used, $\epsilon_{pl}^{[jam]}$ is the one without defense under jamming. Fig. 3 compares the performance of bi-directional path discovery among the three types of mesh jammers for the first path in 10 different configurations over 600x600 square meters of area. Due to its similar trends, we abbreviate the simulation result over 300x300 square meters of area.

Without distinct dependency on the mesh jammer type, the bi-directional path discovery noticeably recovered more paths in some cases such as the configuration #3, #5, #6, and #8. With PREQ jammer in the configuration #1, it found shorter paths. This is because the discovered shorter paths tending to cross the jammed area, not to detour. However, it is obvious that this defense incurs additional overhead such as retransmission and path discovery time although we do not address in this study. Moreover, there exist some issues to apply this mechanism to the existing protocol.

When should the reverse path discovery be triggered? The destination node may be able to trigger the reverse path discovery procedure by sending newly defined *sub-PREQ* frame when it receives the original PREQ from the source node.



(a) Path discovery probability change - bigger markers are ϵ_{pd} after using bi-directional path discovery.



(b) Path length expansion - smaller values of $\delta_{pl}^{[bdp]}$ than 1 indicate that the defense mitigates the jamming effect.

Fig. 3: Performance of bi-directional path discovery under jamming on 10 different configurations (600x600)

This, however, means that the bi-directional path discovery cannot recover paths, unless the original PREQ frames are successfully delivered to the destination[2]. If there is a root node in the MBSS, the source can ask the root node to send reverse path discovery request to the destination upon the assumption that all the communications between each mesh node and the root node are not jammed.

After the reverse path discovery is triggered, how should intermediate nodes forward sub-PREQ and sub-PREP frames? Since intermediate nodes update their forwarding table while they forward mesh frames, they should defer the forwarding table update by reverse path discovery until the source decides the path discovered by the reverse path discovery procedure is better than one discovered by original path. If it turns out that the former is better than the latter, the source should notify all the nodes along the former path to update their forwarding table according to the reverse path discovery. This procedure will also consume extra time and energy.

V. Conclusion

We analyze the jamming effect on the path selection methods in the IEEE 802.11s WLAN mesh standard. We define mesh jamming as an intelligent jamming attack which can efficiently degrade wireless mesh networks, and we compare the effect of conventional jamming and mesh jamming in our wireless mesh network simulator. Our results show that mesh jamming can be more devastating than conventional jamming while it saves attacking cost by selectively jamming a certain type of frames. Based on the trends we observed in the attack simulation, we propose a proof-of-concept defense. Our results show that our defensive techniques provide greater robustness to attack than the HWMP protocol. We will address more practical considerations to apply our defense mechanisms to the existing protocol and improve their effectiveness in future work.

[2]This probability will be of course small because PREQ is relatively resilient to jamming as revealed in our analysis.

References

[1] *IEEE Std 802.11s-2011, Amendment 10: Mesh Networking*, IEEE Computer Society Std.

[2] Z. Ye, S. Krishnamurthy, and S. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 1, Mar.-Apr. 2003, pp. 270–280 vol.1.

[3] J. Lessmann, M. Schoeller, and F. Zdarsky, "Rope ladder routing: Position-based multipath routing for wireless mesh networks," in *World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a*, Jun. 2010, pp. 1–6.

[4] P. Tague, D. Slater, G. Noubir, and R. Poovendran, "Quantifying the impact of efficient cross-layer jamming attacks via network traffic flows," Network Security Lab (NSL), University of Washington, Tech. Rep., 2009. [Online]. Available: http://www.ee.washington.edu/research/nsl/papers/TR005.pdf

[5] A. Wood, J. Stankovic, and S. Son, "Jam: a jammed-area mapping service for sensor networks," in *24th IEEE Real-Time Systems Symposium, 2003. RTSS 2003*, Dec. 2003, pp. 286–297.

[6] H. A. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, "Short paper: Jamming-resilient multipath routing leveraging availability-based correlation," in *Proceedings of the fourth ACM conference on Wireless network security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 41–46.

[7] M. Kim and K. Chae, "Dmp: Detouring using multiple paths against jamming attack for ubiquitous networking system," *Sensors*, vol. 10, no. 4, pp. 3626–3640, 2010.

[8] C. Perkins, E. Belding-Royer, and S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*, IETF Std., Jul. 2003.

[9] A. Vlavianos, L. Law, I. Broustis, S. Krishnamurthy, and M. Faloutsos, "Assessing link quality in ieee 802.11 wireless networks: Which is the right metric?" in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, Sep. 2008, pp. 1–6.

[10] W. T. Tan, P. Hu, and M. Portmann, "Experimental evaluation of measurement-based sinr interference models," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Jun. 2012.

[11] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, ser. MobiCom '10. New York, NY, USA: ACM, 2010, pp. 1–12.

[12] The open80211s project. [Online]. Available: http://open80211s.org/

[13] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*. Artech House, Inc., 2004, ch. 2.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, ser. MobiHoc '05. New York, NY, USA: ACM, 2005, pp. 46–57.

[15] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *Dependable and Secure Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 101–114, Jan.-Feb. 2012.

[16] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: reactive jamming in wireless networks: how realistic is the threat?" in *Proceedings of the fourth ACM conference on Wireless network security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 47–52.