Wormhole Detection Using Channel Characteristics

Shalabh Jain, Tuan Ta, John S. Baras
Institute for Systems Research
University of Maryland, College Park, MD 20742
Email: {shalabh, tta, baras}@umd.edu

***Abstract*—The potential applications and pervasive nature of mobile ad-hoc networks (MANETs) has made them an attractive target for attackers. The wireless medium of communication coupled with constrained resources enable attacks which can be executed by a weak adversary. A wormhole is one such attack which poses considerable threat, particularly to routing protocols. In this paper, we devise a novel scheme for detecting a wormhole by utilizing the inherent symmetry of electromagnetic wave propagation in the wireless medium. We demonstrate the loss of this symmetry in case of a wormhole attack and propose a method to detect and flag the adversary. We modify the insecure neighborhood discovery to incorporate authentication. We further extend this scheme to a trust system with low overhead.**

I. Introduction

Over the past decade, there has been a drastic increase in demand for ubiquitous connectivity. Several important applications, such as monitoring the health of humans, integrity of civil structures, military surveillance and battlefield logistics require robust and distributed sensory capabilities. To keep costs low, the devices used often have limited processing, battery and communication resources. These constraints, coupled with lack of fixed infrastructure, spawn a new class of unsolved problems in wireless networks.

A critical requirement from the nodes in such mobile ad-hoc networks (MANETs), is to be able to cooperate to enhance communication and computation capabilities. However, cooperation over the wireless medium also provides adversaries with the opportunities to launch powerful attacks, even when restricting their activities to a small part of the network. An excellent overview of some popular attacks in MANETs and their countermeasures can be found in [1].

One particularly damaging attack is the wormhole attack, which can be launched by a pair of collaborating nodes. In this attack, two adversarial nodes create a low latency out-of-band link (wormhole), either via external hardware or tunneling through network nodes. The attackers thus provide a path with low hop count. Typical MANET routing algorithms, such as AODV and DSR, select such links for routing, allowing the adversary to draw large amounts of network traffic. Such high traffic links under adversarial control can cause significant leakage of network secrets, performance degradation and congestion in the network. As a result, there is significant research interest in detection of such wormholes [2], [3], [4], [5], [6], [7], [8]. Typical methods use specialized hardware [2], [8], timing based checks [5], [7], or statistical checks based on logical connectivity [4].

In this paper, we present an efficient and robust method for detecting wormholes using the channel state information (CSI) between the communicating nodes. Typically, the variations in the state of the common channel, as seen by a pair of nodes, are similar. Utilizing this property of the wireless channel to generate a secret key for cryptographic purposes has been a well studied topic in literature, [9], dating back to 1995. We claim that presence of adversarial relays, acting as a wormhole, can destroy this symmetry. We formulate a method to detect this loss of symmetry. Estimation of the CSI is needed for coherent demodulation in most communication systems. Many commercial products support simple software routines to obtain the CSI, typically as the received signal strength (RSS). Therefore, our scheme can be added on to the current systems without hardware modifications. In addition, since our scheme does not rely on any special beacon or signals, it can be used with regular data transmission, without much overhead.

The rest of the paper is organized as follows. In section II, we describe the typical wormhole attack followed by our system assumptions in section III. In section IV, we describe the extraction of bits from the channel state. In section V, we propose methods to use the bit sequence for security. In section VI, we evaluate the performance of our scheme, using both MATLAB and our testbed.

II. Wormhole Attack

A typical wormhole scenario is shown in Figure 1. Consider the nodes to be distributed over an open area. Nodes A_1 and A_2, represent adversarial nodes that create a low latency tunnel. The tunnel L_1 represents a direct link created using external hardware, such as powerful directional antennas. The link L_2 represents a tunnel created by encapsulating the original messages received by A_1 and forwarding them to A_2 through non-adversarial nodes that are a part of the network. The adversary A_2 then re-broadcasts the encapsulated message as the source.

Routing protocols designed for MANETs, such as AODV select low hop count paths. In the scenario in Figure 1, routes from $S_1 \dots S_5$ would all use the wormhole to route packets to $D_1 \dots D_4$.

There exist different classifications of wormholes based on the adversarial behavior. The survey [3] provides an excellent taxonomy of different wormholes. Here we briefly enumerate the relevant features and behavior required for our presentation.

978-1-4577-2053-6/12/$31.00 ©2012 IEEE

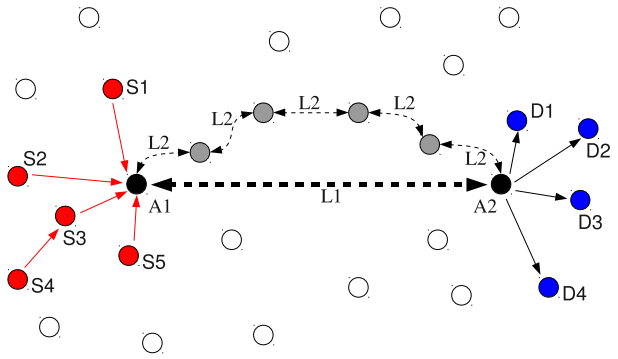


Fig. 1. A typical distribution of nodes in a MANET. L1 represents the wormhole link using external hardware. L2 represents the wormhole link created tunneling through nodes genuinely a part of the network.

A wormhole may be hidden or visible, depending on whether the adversarial nodes announce themselves to the network. A hidden wormhole manifests itself only through its actions. If Figure 1 represents a hidden wormhole, nodes A_1 and A_2 will be invisible to the network. Thus S_1 and D_1 will appear as one-hop neighbors.

Typically the adversaries creating the wormhole are assumed to be simple relays, capable of capturing the messages but not altering it. It is precisely this property which makes wormhole impossible to be detected by cryptographic techniques. A more powerful adversary may be one where the node can selectively modify the messages before re-broadcasting. However, there are several upper layer techniques to preserve the integrity of the transmitted messages. Additionally, such adversaries would need to buffer packets before making any changes. This cause significant timing overhead which can be detected. A good analysis of the effect of speed on adversarial behavior is presented in [10].

Previously studied wormhole detection techniques are based on higher layer (network, MAC) metrics. Such metrics are highly dependent on network architecture, traffic load and contention management mechanism. Several of these schemes also require specialized hardware or hierarchy among nodes. Our scheme utilizes physical layer characterestics of the point-to-point link. Thus, it is independent of variations induced by the network. This adds a new dimension of robustness. Additionally, we use a flat network structure and require no specialized hardware.

III. System Assumptions

Since our scheme uses channel characteristics, there exist certain channel requirements for our scheme to work successfully. We assume the channel between any pair of nodes to be symmetric and Rayleigh block fading, with fading duration larger than the round trip time (RTT) between the nodes. The scheme can tolerate temporal variations in the channel parameters that are bounded by the quantization step. As we will highlight later, the quantization step size is a design parameter within our scheme, which can be optimized based on the deployment environment. We find that these channel assumptions hold reasonably well in case of static sensor networks, or mobile nodes with slow movements.

Our scheme operates independent of the higher layer MAC and routing protocols. We assume the existence of some form of contention management scheme for access to the wireless channel. For authentication during neighborhood discover phase, the scheme will perform well with any MAC and higher layer protocol. However, to build trust systems, we require the packet reception to be acknowledged. Thus, any MAC protocol which ensures instant feedback after packet reception will suffice, for example, the 802.11 MAC.

We assume the adversarial behavior to be limited to relaying and any offline attacks. In case of a relay with the capability to modify the packets, we can couple our scheme with any higher layer protocol used to ensure integrity of the messages in the network. For example, any form of a message authentication code will serve this purpose. It should be noted that hidden wormholes typically cannot be thwarted by higher layer cryptographic schemes. The benefits of our scheme thus complement the higher layer cryptographic methods, not overlap.

IV. Bit Extraction

The wireless channel, while being the source of problems, can also provide a good source of randomness to be used in cryptographic key generation. Several previous works, [9], [11], [12], [13], have focused on extraction of a key from the channel measurements. Since most coherent detection schemes utilize some form of pilots to estimate the channel, these schemes have the advantage of adding little overhead to the communication system.

Typically, pilot symbols are inserted to aid channel estimation. There exists a wide array of literature concerning optimal allocation and placement of pilots, as well as channel estimation techniques. The work of Tong, et al., [14], is an excellent example. Consider the case where the pilot symbols $\mathbf{p}$, are inserted in the middle of the block (similar to the GSM packets). Let the observations of those pilot symbols be $\mathbf{y_p}$. The MMSE channel estimate is simply

$$\hat{h} = \frac{1}{|\mathbf{p}|^2}\mathbf{p}^H\mathbf{y_p}.$$

The estimate, $\hat{h}$, can then be quantized for the purpose of generating a sequence of random bits. We discuss two schemes [11] and [13], for generating the bit sequence for our purpose.

Since our intent is not to use the sequence as key for cryptographic purpose, we may relax certain requirements and simplify the existing schemes. Firstly since in the wormhole case, the sequence is not reused and the adversary does not act directly on the key, the bit sequence generated need not be uniform. Secondly, since we are using correlation rather than perfect matching, the sequences generated need not be identical.

A. Bit Extraction Using Phase Of Channel State

In [13], the authors use the phase of $\hat{h}$ to derive a bit sequence. Assuming the channel fading parameter has a Rayleigh distribution, the phase is distributed uniformly over $[-\pi, \pi]$. Thus it is a good choice for generating random bits. Even in slow fading channels, there can be rapid fluctuations in the phase. This is advantageous, as it increases the rate of bit generation. However, it can be a source of asymmetry and error as well. To generate the bits, we simply quantize the phase $\hat{\phi} = \arctan \frac{imag(\hat{h})}{real(\hat{h})}$, using an L-bit uniform quantizer Q.

$$\{b_1, b_2, \ldots b_L\} = Q(\hat{\phi}).$$

In practical scenarios, there may be a certain degree of correlation between the generated bits. We however do not employ any decorrelation mechanism here. For our scheme, we can accommodate this correlation during the matching phase by selecting conservative thresholds.

B. Bit Extraction Using Magnitude Of Channel State

Most commercially available radios today do not provide direct access to the phase of the channel estimate. Instead they provide the received signal strength indicator (RSSI), which can be considered as a measure of the magnitude of the channel response. In [11], the authors provide a simple scheme for deriving a bit sequence by using a non uniform, L-bit quantizer Q' to detect deep fades. Here

$$\{b_1, b_2, \ldots b_L\} = Q'(|\hat{h}|^2) \approx Q'(RSSI).$$

The authors of [11] show that even by considering $L = 1$, i.e., binary quantization, the best that the adversary can do is to predict the Hamming weight of the generated sequence. In the simplest scenario, the quantizer reduces to

$$RSSI \gtrless_0^1 q,$$

where the threshold q can be optimized for performance. Typically q represents the mean of underlying distribution of the channel state, which can be assumed to be known before hand, or determined adaptively as the sample mean. We can also use a moving average filter to represent the threshold. It can be observed that regardless of the update scheme, the bit sequence generated at both ends would be similar. We will highlight the effect of q during the performance evaluation of our scheme.

Intuitively, the magnitude provides a more natural and robust mechanism for generating the bits. However, it suffers from a major disadvantage when the channel is slow fading. The bits in the sequence may not have sufficient variation to effectively utilize the independence of the channels in the presence of an adversary. Thus, we may not be able to extract a meaningful bit sequence, leading to a high probability of missed detection.

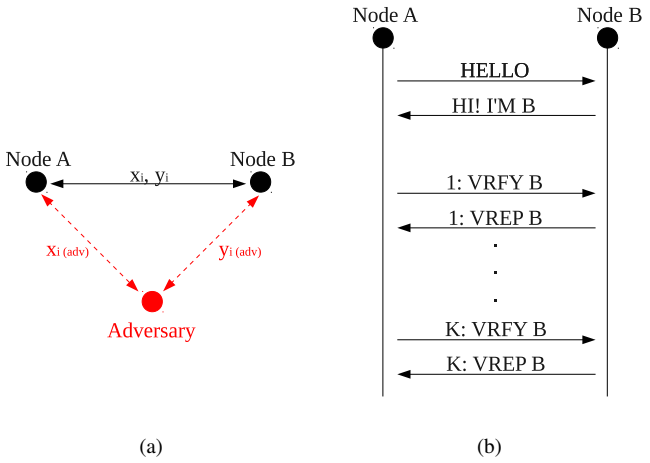


Fig. 2. (a) Scenario of bit sequence extraction with (red) and without (black) adversary (b) A timing flow diagram of the modified neighborhood discovery protocol

V. Security Scheme

Consider the Figure 2(a). Let x_i and y_i be the sequence of bits extracted by nodes A and B respectively, during the ith message exchange using one of the methods highlighted in section IV. Let x_i^{adv} and y_i^{adv} be the corresponding bit sequences in the presence of an adversary. We utilizes the fact that the channel between A and the adversary is independent of the channel between B and the adversary. Thus, the bits sequences x_i^{adv} and y_i^{adv} would yield a lower correlation when compared to x_i and y_i.

These sequences can be used to detect wormholes either initially during neighborhood discovery (or route discovery), or over the entire duration of transmission as a trust metric. The former incurs a penalty of a few packets, depending on the quantization levels. Since the overhead of the actual scheme is minimal, utilizing it over several data packets forms a robust low cost metric.

A. Trust Metric

In this scheme, we consider the case where the route discovery mechanism proceeds without any security and selects the wormhole link. During actual data transmission, for each packet received by B from A, it extracts y_i. To minimize overhead, we select a single bit to be transmitted back to A, along with the ACK. The least significant bit may be poor choice since it is most prone to error due to channel variations. On the other hand, the most significant bit exhibits excessive robustness to quantization errors in the presence of an adversary, thus reducing security. We can select the middle order bit, $y_i^b = (y_i)_{\frac{L}{2}}$. This can be re-transmitted to A with the ACK reply, which enables A to compute the corresponding x_i^b. In case of an adversary capable of modifying the packets, this bit can be cryptographically secured with rest of the data.

Define t_i to be the trust value learned from the ith packet. $t_i = 1$ if $x_i^b = y_i^b$, and 0 otherwise. Thus assuming that the channel states over different packets are independent, t_i will

be an i.i.d Bernoulli random variable. Let p be the probability that $t_i = 1$ in case there is no adversary, and p^{adv} be the probability that $t_i = 1$ in the presence of an adversary.

Consider that the system evaluates its path selection strategy to check for adversaries after N packets. Thus the accumulated trust, $T = \sum_{i=1}^{N} t_i$, will have a Binomial distribution with the parameters p or p^{adv}. Based on the accumulated trust, we can make our decision as

$$T \gtrless_{adv}^{noadv} N_0,$$

where N_0 can be optimized on the basis of an α-level test. For security, our intent is to minimize the probability of missing an adversary. Let us define α_m to be the acceptable probability of missed detection. Such criteria leads to a penalty in the probability of false alarm. However, if we consider a MANET to be densely connected, a wrongly flagged path will lead to very little overhead in terms of connectivity or latency.

We may select N_0 as

$$N_0 = \arg\min_j \left(1 - f(N, j, p^{adv})\right) \leq \alpha_m, \tag{1}$$

where $f(N, j, p)$, denotes the binomial cumulative distribution function.

B. Neighbor Discovery

This scheme is intended to detect a wormhole during neighborhood discovery with a one time packet repetition cost. Consider the scenario where a node A wishes to perform neighborhood discovery (ND). Typically, a node would send out HELLO messages and wait for the reply from its neighboring nodes. We modify this method as shown in Figure 2(b). After receiving the initial reply, the node A sends out K verification messages (VRFY), receiving a reply (VREP) from the neighbors each time. The VRFY and VREP packets require no special structure, just the basic pilot symbols to perform channel estimation. Thus we use the minimum size packets permitted by the protocol MAC as our verification packets.

With each reply, node B appends the extracted bit sequence y_i. This enables node A to compute x_i. Consider

$$X = x_0||x_1|| \cdots ||x_K,$$

and

$$Y = y_0||y_1|| \cdots ||y_K.$$

Thus the decision of security may be made by the node A as

$$\sum_j \mathbb{I}(X^j = Y^j) \gtrless_{adv}^{noadv} \tau,$$

where $\mathbb{I}(.)$ represents the indicator function and X^j, Y^j represent the ith bit of the sequence X and Y respectively. The value of τ can be optimized based on the significance level tests as shown in the previous section.

VI. Simulations

We evaluate the performance of the proposed mechanism using both MATLAB simulations and RSSI measurements from our sensor testbed. Since our scheme utilizes physical layer properties of the wireless channel, rather than network specific metrics, it is independent of the network architecture. Therefore, it suffices to demonstrate the validity of our claims by considering the channel between a single transmitter and receiver pair for the non-compromised case, and the presence of a single adversarial node for the compromised case.

In the initial experiments, we use simple binary quantizers with static quantization levels. We then study the effect of quantization, by varying the number of static quantization levels. We also present authentication results for the scenario where the system is not aware of the channel characteristics. In this case, we use adaptive quantization, where the quantization level is computed as the sample mean.

A. MATLAB Simulations

In our simulations, we use a conservative channel model to demonstrate the robustness of our scheme. We tighten our assumptions about channel symmetry and independence, as compared to those in literature work on secret key generation. We do not consider the channel between the transmitter and receiver to be perfectly symmetric; rather highly correlated. In the adversarial case, we do not assume the channels from the adversary to the transmitter and the receiver to be independent; rather they exhibit a lower correlation than the non-compromised case. Let ρ_{adv} be the correlation between the Gaussian components of the complex channel gain in the adversarial case. Let ρ_{sym} be the corresponding parameter in non-adversarial case. We present our system performance for $\rho_{adv} \leq 0.7$, and $\rho_{sym} \geq 0.8$.

For a robust detection mechanism, the probability of missed detection, α_m, must be reasonably low. For our simulations, we use a value of 1%, i.e. $\alpha_m = 0.01$. Recall that p and p^{adv} denote the probabilities that the response bit extracted from the receiver channel is equal to the verification bit extracted from the transmitter channel in the non-adversarial and adversarial cases, respectively. We evaluate the decision threshold N_0/N for our channel models, which depends on α_m and p^{adv}. The value of p^{adv} can be calculated accurately, based on the method of bit sequence generation and channel parameters. For example, when generating the bit sequence from the magnitude of the channel response, we can use the bivariate Rayleigh distribution [15].

Due to complexities involved in analytical evaluation, we use simulations to compute the value of p^{adv}. We perform simulations considering $SNR = 10dB$. We observe, for $\rho_{adv} = 0.7$, the parameter $p^{adv} = 0.68$ when using the magnitude, and $p^{adv} = 0.74$ when using the phase. Based on the equation (1), we find $N_0 \sim 0.7N$ and $N_0 \sim 0.8N$ to perform well for the bit generation using magnitude and phase respectively. In other words, if 70% of the received bits match, we can conclude the absence of an adversary with high confidence.

In Figures 3, 4, we plot the probability of declaring a link to be non-adversarial, as a function of the number of observed packets. We consider a pilot aided channel estimation scheme, using 16 pilots inserted in the middle of the frame. We demonstrate the robustness of our scheme even in noisy channel conditions with $SNR = 0dB$.

The performance using the phase of the estimated channel state to obtain the bit stream, is shown in Figure 3. As the phase is uniform in $[-\pi, \pi]$, we fix the quantization level at $q = 0$ and obtain a single bit from each estimate. The sensitivity of our scheme on the quality of channel estimation can be clearly seen from Figure 3(a). At low SNR, since the channel estimation is noisy, we require almost twice the number of packets required for the case of $SNR = 10dB$. Comparing Figures 3(a) and 3(b), we can observe the performance variation with correlation. For reasonable correlation, when $\rho_{sym} - \rho_{adv} > 0.2$, the probability of false alarm declines rapidly to a low value. Even for extremely matched correlation values, as in 3(b), the scheme performs reasonably well, though at an added cost of sensing time. However, since the computation and power overhead of the scheme is limited, long sensing times do not penalize our network much. In such conditions however, it would be difficult to use our scheme for authentication during the neighborhood discovery phase.

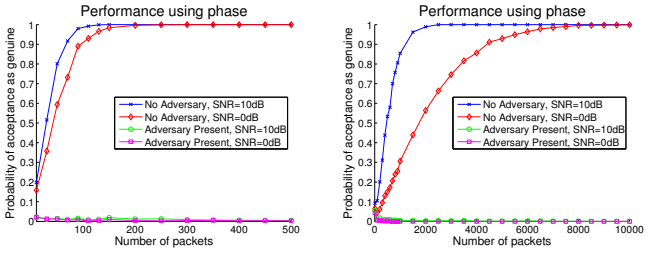


Fig. 3. Bit stream generation using phase of the estimated channel state (a) $\rho_{adv} = 0.5$, $\rho_{sym} = 0.9$; (b) $\rho_{adv} = 0.7$, $\rho_{sym} = 0.8$

For Figure 4, we use the magnitude of the estimated channel state to obtain the bit stream. Since the channel model in our simulations is sufficiently time varying, performance using the magnitude is similar to using the phase. In generating Figure 4, we use adaptive quantization. Here, we assume no prior knowledge of the CSI distribution. We set the quantization level equal to the sample mean. This method models the realistic scenario where the sensors do not have prior knowledge about the environment they are deployed in. We observe that adaptive quantization performs equally well, when compared to static quantization. This is intuitive, since our scheme relies on symmetry. The sample means, though different from the true mean will be symmetrically computed.

In Figure 5, we highlight the effect of quantization size on robustness. Here, we ignore the system overhead, and use all of the generated bits for authentication. The binary quantization considered previously, though robust, requires a long time to reach a confident decision. Increasing the

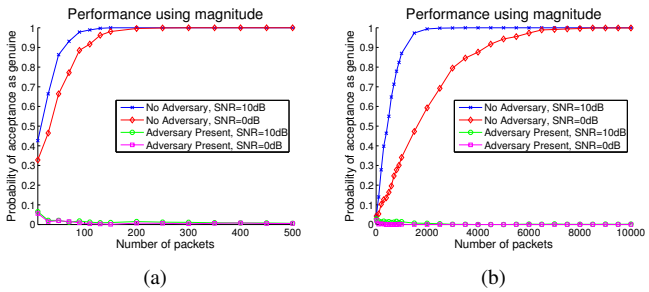


Fig. 4. Bit stream generation using magnitude of the estimated channel state with adaptive quantization levels (a) $\rho_{adv} = 0.5$, $\rho_{sym} = 0.9$; (b) $\rho_{adv} = 0.7$, $\rho_{sym} = 0.8$

number of quantization levels can lead to several fold increase in the rate of the generated bits. However, an increase in bits per sample also increases sensitivity to minor losses in symmetry. We consider a 4- and 8-level uniform quantizer for a Rayleigh channel. To minimize errors due to minor changes in the channel, we use Gray code for encoding the quantizer output. It can be seen from Figure 5 that for quantizing the magnitude of the channel state, increasing the quantization levels to 8, even though increases bit generation rate, decreases performance.

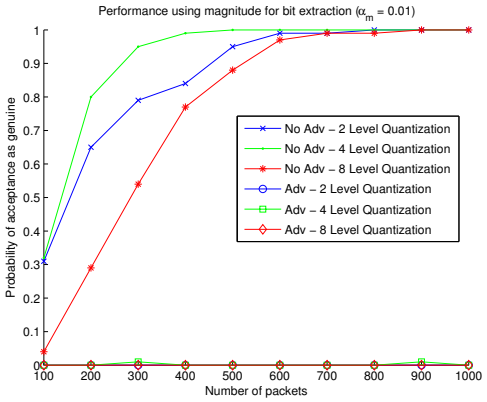
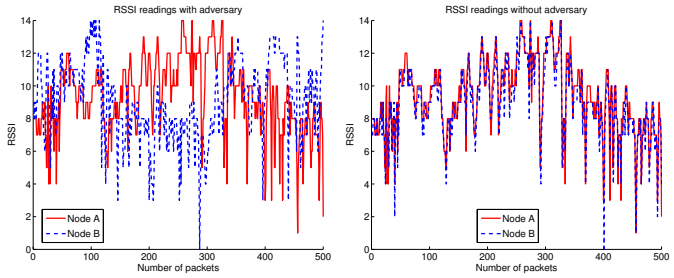


Fig. 5. The effect of quantization of the magnitude on security

B. Performance Evaluation Using Sensor Testbed

We implement our scheme on an IRIS Mote sensor testbed to evaluate its performance. We use the TinyOS programming environment to interface with the motes. Like most commercial wireless hardware, the IRIS mote provides the quantized RSSI readings which can be used for generation of a bit sequence for security. We conduct experiments for the limited mobility (walking speed) and stationary case. Figures 6(a) and 6(b) display the variation of RSSI readings over 500 samples, as recorded by the transmitting and receiving sensors, in the presence and absence of an adversary respectively. We can clearly observe the low (and high) correlation between the variations in the adversarial (and non-adversarial) case. Thus,

we can verify that even with mobility, our assumptions while designing the system hold true.



(a) (b)

Fig. 6. RSSI readings of transmitting and receiving IRIS motes for (a) adversarial scenario; and (b) non-adversarial scenario

We implement our algorithm on the IRIS motes using the sample mean for quantization. In Figure 7, we plot the probability of declaring the link free from any adversarial action, as a function of number of exchanged verification packets between the nodes. In a practical scenario, where we are unaware of the channel conditions, it is impossible to accurately calculate the N_0/N ratio. In Figure 7, we highlight the effect of the ratio on system performance. We observe that a ratio of $N_0/N \in [0.75, 0.8]$ yields a good tradeoff between probability of missed detection and false alarm. We can observe that even with 50 packets, we achieve a false alarm rate less than 10%, which is tolerable for most practical networks.

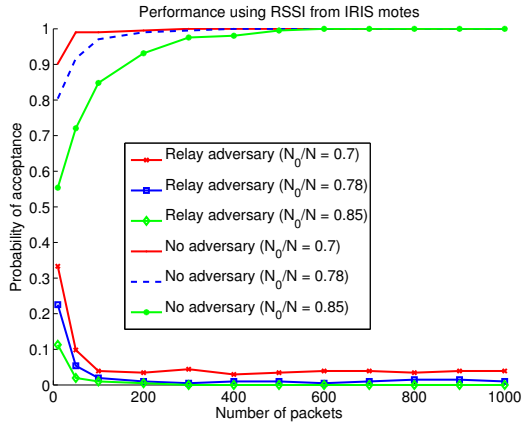


Fig. 7. Performance of wormhole detection scheme for varying N_0/N ratios on IRIS sensor motes, using RSSI

VII. Conclusion

In this paper we described a practical low cost method to detect wormhole attack using the inherent symmetry in the wireless channel. We analyzed two characteristics of the channel response, phase and magnitude, that can be used as indicators in our security scheme. We demonstrated that channel measurements from IRIS sensor motes support our assumptions on channel characteristics. We further show through MATLAB simulations and IRIS sensor testbed that our scheme achieves wormhole detection probability close to 1 after a suitable number of verification packets.

Acknowledgment

This material is based upon work partially supported by the Defense Advanced Research Projects Agency (DARPA) through contract award number 013641-001, MURI grant award W911-NF-0710287 from the Army Research Office, MURI grant award 015356-001 from the AFOSR and grant award CNS1018346 from the National Science Foundation (NSF).

Any opinions, findings and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of any of the funding agencies mentioned.

References

[1] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, ser. Signals and Communication Technology. Springer, US, 2007, pp. 103–135.

[2] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proc. 2003 IEEE Infocom*, vol. 3, 2003, pp. 1976–1986.

[3] I. Guler, M. Meghdadi, and S. Ozdemir, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," *IETE Technical Review*, vol. 28, no. 2, pp. 89–102, 2011.

[4] S. Zheng, T. Jiang, J. Baras, A. Sonalker, D. Sterne, R. Gopaul, and R. Hardy, "Intrusion detection of in-band wormholes in MANETs using advanced statistical methods," in *Proc. 2008 IEEE Milcom*, Nov. 2008, DOI: 10.1109/MILCOM.2008.4753177.

[5] H. S. Chiu and K.-S. Lui, "DelPHI: Wormhole detection mechanism for ad hoc wireless networks," in *2006 1st International Symposium on Wireless Pervasive Computing*, Jan. 2006.

[6] Y. Xu, G. Chen, J. Ford, and F. Makedon, "Detecting wormhole attacks in wireless sensor networks," in *Critical Infrastructure Protection*, ser. IFIP International Federation for Information Processing, E. Goetz and S. Shenoi, Eds. Springer, Boston, 2007, vol. 253, pp. 267–279.

[7] P. V. Tran, L. X. Hung, Y.-K. Lee, S. Lee, and H. Lee, "TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks," in *Proc. 2007 Consumer Communications and Networking Conference*, Jan. 2007, pp. 593–598.

[8] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. 11th Network and Distributed System Security Symposium*, 2004, pp. 21–30.

[9] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3 –6, Jan. 1995.

[10] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Towards provable secure neighbor discovery in wireless networks," in *Proc. 6th ACM Workshop on Formal Methods in Security Engineering*, 2008, pp. 31–42.

[11] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conference on Computer and Communications Security*, 2007, pp. 401–410.

[12] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM International Conference on Mobile Computing and Networking*, 2008, pp. 128–139.

[13] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. 2011 IEEE Infocom*, Apr. 2011, pp. 1422 –1430.

[14] L. Tong, B. Sadler, and M. Dong, "Pilot-assisted wireless transmissions: general model, design criteria, and signal processing," *IEEE Signal Processing Magazine*, vol. 21, no. 6, pp. 12 – 25, Nov. 2004.

[15] K. T. Hemachandra, "A mathematical framework for expressing multivariate distributions useful in wireless communications," M.Sc Dissertation, University of Alberta, Canada, Apr. 2011.