International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2827-2830 ISSN: 2249-6645

A Novel Method for Preventing Selective Jamming Attacks in Wireless Networks

Ashrafunnisa[1], G. Sridevi[2]
[1]M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.
[2]Assoc. Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.

ABSTRACT: *Wireless networks are susceptible to numerous security vulnerabilities due to the open nature of the wireless medium. Anyone with a transceiver can eavesdrop on ongoing transmissions, block the transmission of legitimate ones or inject spurious messages. One of the fundamental ways for degrading the overall network performance is by jamming wireless transmissions. In this paper, we deal with the problem of selective jamming under an internal threat model. Here the eavesdropper who is aware of network secrets and the implementation details of all the layers of network protocols in the network stack. The attacker uses his/her internal knowledge for launching selective jamming attacks in which high importance messages are targeted. Hence we propose a novel method for preventing selective jamming attacks in wireless networks.*

Keywords: *All- or- nothing transform, Jamming, SHCS.*

I. INTRODUCTION

Wireless networks are prone to diverse set of attacks due to the nature of its shared medium. Well-designed network architectures may address several security threats [1][2][3]. However, wireless networks are even sensitive to number of security attacks. From the existing security attacks to be resolved, we kept our centre of interest on Selective Jamming (Figure 1) which is the recent headway on the bad side of technology. We do have various traditional jamming attacks like random jamming, constant jamming, deceptive jamming etc [4][5]. To have any of these attacks, the attacker has to spend more vigor but the impact on the network degradation is less. Moreover, there are wide varieties of techniques to prevent such several traditional jamming strategies in [6].

But, in Selective Jamming, the attacker will expend fewer resources and can create drastic bad consequences. Taking this as ground principle, we can assign a tagline for the selective jamming as "less effort, more impact" method. The attacker who does the selective jamming will target on specific sender node (SN) and receiver node (RN) and thereby corrupt only the significant packets (e.g. Route REQ / REPLY, ACK) that travel between them. Selective jammer (SJ) node will use packet classification methods [7] to know whether the packet is significant or not. To achieve this selective jamming attack, the jamming node should be an internal part of network which makes it to know all the networks secrets in an easier way. Finally, all these things make attacker to perform selective jamming with less energy consumption.

In this paper, we deal with the problem of selective jamming under an internal threat model. Here the adversary who is aware of network secrets and the implementation details of all the layers of network protocols in the network stack. The attacker uses his/her internal knowledge for launching selective jamming attacks in which high importance messages are targeted. For example, a jammer can target TCP acknowledgments in a TCP session or target route request or reply messages at the routing layer.

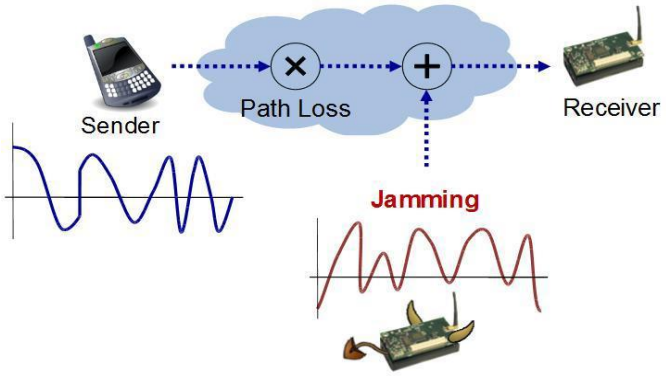

Figure 1: Jamming in wireless network

II. RELATED WORK

Selective jamming problem has been addressed under various threat models. The impact of external selective jammers targeting various control packets at the MAC layer is studied in the paper [8] by author Thuente. Selective jamming attack is based on protocol semantics, where they considered several packet identifiers for enciphered packets such as packet size, signal sensing and timing information of different protocols. Unification of packet characteristics like minimum length and the inter packet timing was used in order to prevent selectivity. In [9], the authors attempts to make use of protocols at

various layers to get three advantages- targeted jamming, jamming gain, and reduced probability of detection. In targeted jamming attack, it may jam particular nodes, flows or links. Here the adversary may be interested in specific parts of the network and attacking those regions can lead to further jamming gains, where as in reduced probability of detection, the sufferer network may not be aware of jamming attack counter measures.

Selective jamming attacks have been experimentally implemented using the software defined radio engines [10]. USRP2-based jamming platform called RFReact was implemented in [10] that enables selective and reactive jamming. We develop 3 schemes that prevent jamming attacks: they are Strong Hiding Commitment Scheme, Cryptographic Puzzle Hiding Scheme and All or Nothing Transformation.

III. PROPOSED WORK

A. Problem Statement

Lets consider Figure 2 where A(alice) and B(bob) are communicating through a wireless network and "j" is jamming node whenever alice sending some packets m to bob. Node "j" will classify m and get first few bytes then adversary "j" corrupt them beyond the recovery and add them when received by Bob. The main objective is to prevent attackers who are going to do selective jamming attacks on our network.

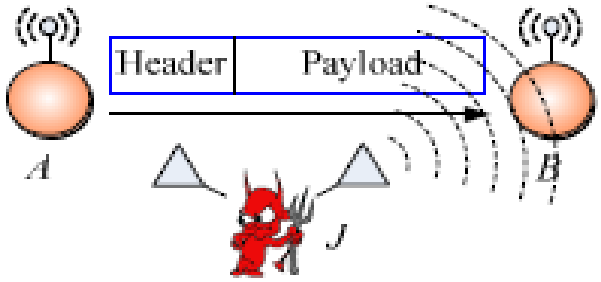

Figure 2: Realization of a selective jamming attack

Figure 3 shows the generic format for a wireless Physical header contains information regarding the length of frame and transmission rate in MAC protocol, source, destination field, MAC header is followed by frame body that contains IP datagram.

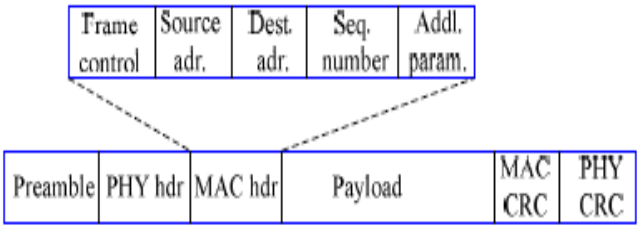

Figure 3: A generic frame format for a wireless network

B. Strong Hiding Commitment Scheme (SHCS)

Strong Hiding Commitment Scheme (SHCS) which is based on asymmetric cryptography. Our main goal is to satisfy the strong hiding property by keeping the computation overhead to a minimum. A commitment scheme allows an entity "S", to commit to a chosen value, to another entity "V" while keeping that value hidden to others. Commitment scheme must satisfy the following two properties:

- **Binding:** Deliver the committed value to the receiver end, here the sender cannot alter the value once it is committed
- **Hiding:** The receiver cannot see the message until he gets the secret key, after receiving the key receiver verifies that it is indeed the message to which the sender is committed.

Here the role of the committer is implicated by the sender or transmitting node, whereas role of the verifier is implicated by any receiver including the attacker. Consider that sender S has a packet "m" for the transmission for receiver R. First, before transmission S constructs the following:
(C,d) = commit (m)
C= Ek (π1(m)) and d=k

Where "Ek" the commitment function is an asymmetric encryption algorithm (eg. DSA or RSA [11]), "π1" is a publicly known permutation and k is a randomly selected key. At the receiver end, upon receiving d the receiver R computes m = π1(Dk (C)), where "π1" is the inverse permutation of π1 and also it verifies the signature which is attached to the packets.

C. Cryptographic Puzzle Hiding scheme

A sender "S" has a packet "m" for transmission. The sender selects a random secret key "k" , of a desired length. S generates a puzzle (key, time), where puzzle() denotes the puzzle generator function, and "tp" denotes the time period required for the solution of the puzzle. Parameter is measured in units of time, and it is directly dependent on the assumed computational capability of the attacker, denoted by N and measured in computational operations per second. After generating the puzzle "P", the sender broadcasts (C, P). At the receiver side, any receiver R solves the received puzzle to recover secret key and then computes. Cryptographic Puzzle includes two types of methods.

- Time-lock Puzzles
- Puzzles based on hashing

Time lock Puzzles is based on the iterative application of the precisely controlled number of modulo operations. Time-lock puzzles have several attractive features such as the fine granularity in controlling "tp" and the sequential nature of the computation. Moreover, the Puzzle generation requires significantly less computation compared to the puzzle solving. Computationally limited receivers can incur significant delay and the energy consumption when dealing with modulo arithmetic. In this case, the hiding scheme can be implemented from cryptographic puzzles which employ computationally efficient cryptographic primitives. Client puzzles proposed in, use one way hash functions with partially disclosed inputs to force the puzzle solvers search through a space of a precisely controlled size. In our context, the sender picks a random secret key k with k = k1||k2. The lengths of k1 and k2 are s1, and s2, respectively. He then calculates C = Ek(π1(m)) and transmits (C, k1, h(k)) in this particular order. To obtain key k, any receiver has to perform On average 2s2−1 hash operations (assuming perfect hash functions). Because the puzzle cannot be solved before hash function h (k) has been received, the adversary cannot classify m before the completion of m's transmission.

D. Hiding based on All-Or-Nothing Transformation

In this scheme, the packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform the packet classification until all the pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet "m" is partitioned to a set of "x" input blocks m = {m1, m2, m3….}, which serve as an input to an The set of pseudo messages m = {m1, m2, m3,…..} is transmitted over the wireless link. Recently Rivest motivated by different security concerns arising in the context of the block ciphers, introduced an intriguing primitive called the "All-Or-Nothing Transform (AONT)". All- or- Nothing transform is an efficiently computable transformation "T" on strings such that

- For any string "x", given *all* of T(x), one can efficiently recover "x"
- There exists some threshold value such that any polynomial time adversery that learns all but bits of T(x) obtains no information about "X" (in a computational sense).

Figure 4 shows the proposed AONT- based packet hiding method. The Sender transmits the secret message, which is divided into blocks of fixed size. These blocks are given as input to AONT system. Then AONT system encrypts these message blocks with a shared secret key and then sends to the receiver. Now the receiver decrypts the received blocks with the same key, thus retrieves the original data.

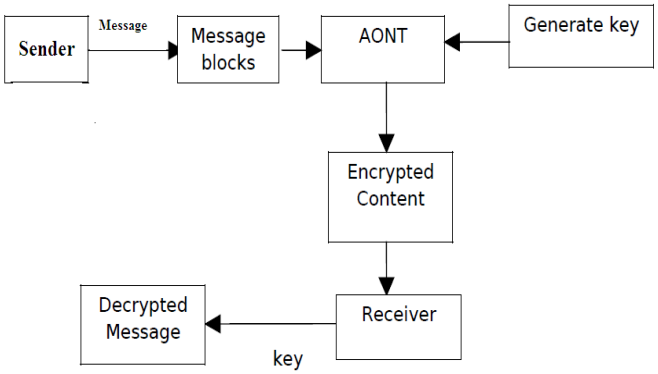

Figure 4: AONT- based packet hiding method

IV. CONCLUSION

There are various categories in wireless networks like sensor network, Ad hoc, WLAN networks. Jamming creates a very bad impact on any of these wireless networks. Specifically, if Selective Jamming is done, the impact is even more serious. Selective jamming is treated as an internal threat model, so it would be difficult to detect it for a normal sender node or receiver node. Here, we have proposed a solution to identify the exact node that is performing selective jamming attack, by initially checking the existence of selective jammer between specific sender and receiver node. Finally, we have given three novel methods to prevent selective jamming by ensuring privacy of the transmitted message.

REFERENCES

[1] B. Potter. Wireless security's future. IEEE Security Privacy Magazine, 1(4):68-72, 2003.
[2] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A secure On-demand routing protocol for ad hoc networks. In 8th ACM International Conference on Mobile Computing andNetworking, pages 12{23, September 2002.
[3] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In Proceedings of IEEE Infocom 2003, pages 1976-1986, 2003.
[4] Wenyuan Xu, Wade Trappe, Yanyong Zhang andTimothy Wood, The Feasibility of launching andDetecting Jamming Attacks in Wireless Networks, MobiHoc‟ 05, May 25–27, 2005.
[5] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys & Tutorials, PP(99):1–13, second quarter 2011.
[6] K. Fazel and S. Kaiser, Multi-Carrier and Spread SpectrumSystems.Wiley, 2003.
[7] Alejandro Proano and Loukas Lazos,Packet-Hiding Methods for Preventing SeleJamming Attacks, IEEE Transactions 2012 on dependable and secure computing, vlo.9, N0.1, 2012
[8] D.Thuente and M.Acharya. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In proceedings of the IEEE Military Communications Conference MILCOM, 2006.
[9] T. X. Brown, J. E. James, and A. Sethi. jamming and sensing of encrypted wireless adhoc networks.In proceedings of MobiHoc, pages 120-130 ,2006
[10] M. Wilhelm, I. Martinovic, J. Schmitt and V. Lenders. Reactive jamming in wireless networks: How realistic is the threat? In proceedings of Wi Sec, 2011.