IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 06, Issue 1, January 2016, ||V-5|| PP 62-67

A Node Based Privacy Approaches for Preventing Selective Jamming In Wireless Networks

[1]Mrs. Thaiyalnayaki S, [2]Dr. A.N. Nanda Kumar, [3]Mr. S. Niresh Kumar,
[1]*Dhanalakshmi Srinivasan College of Engineering and Technology,*
[2]*Dhanalakshmi Srinivasan College of Engineering and Technology,*
[3]*Dhanalakshmi Srinivasan College of Engineering and Technology,*

ABSTRACT: *Wireless networks are still an emerging field in terms of security. Taking advantage from unreliability nature of wireless medium, antagonists can easily accomplish numerous attacks. Among those attacks, spot jamming is more clever technique during which jammer will target and corrupt only the messages of high importance. There are existing methods to prevent selective jamming in internal threat model like strong hiding commitment scheme(SHCS), cryptographic puzzle hiding scheme(CPHS) during which they focused only on the proper message delivery to the receiver node. But on the other side, jammer node can solve the puzzle by taking entire packet, making the adversary to know the secured message that was transmitted. initially, a mechanism to spot the existence of spot jamming is demonstrated. Later, an answer to understand the precise node that's performing spot jamming springs . Then two novel techniques called Embedding Future Key (EFK) and Medial node Method (MNM) are proposed to prevent selective jammi Finally, experiments are conducted on proposed methods and it is established that better throughput is achieved than the existing methods.*

KEYWORDS: *Jamming, Wireless Network*

I. INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. It has been shown to actualize severe Denial-of-Service (DOS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses.

Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high-power interference signals. However, adopting an "always- on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect.

Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit - level protection by spreading bits according to a secret pseudo noise (PN) code known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

SELECTIVE JAMMING

In selective jamming, it addresses the problem of jamming under an internal threat model. Consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly.

In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

PACKET CLASSIFICATION:

To investigate the feasibility of real-time packet classification for launching selective jamming attacks, under an internal threat model. To show that such attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes. Investigate the impact of selective jamming on critical network functions. The findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer.

PREVENTION SCHEMES

To mitigate such attacks, develop three schemes that prevent classification of transmitted packets in real time. The schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. Analyze the security of the schemes and show that they achieve strong security properties, with minimal impact on the network performance.

II. SYSTEM ANALYSIS

EXISTING SYSTEM

To prevent selective jamming in internal threat model like strong hiding commitment scheme(SHCS), cryptographic puzzle hiding scheme(CPHS) during which they focused only on the proper message delivery to the receiver node.

But on the other side, jammer node can solve the puzzle by taking entire packet, making the adversary to know the secured message that was transmitted.

PROPOSED SYSTEM

Selective jamming attacks, the adversary must be capable of implementing a “classify-then-jam” strategy before the completion of a wireless transmission.

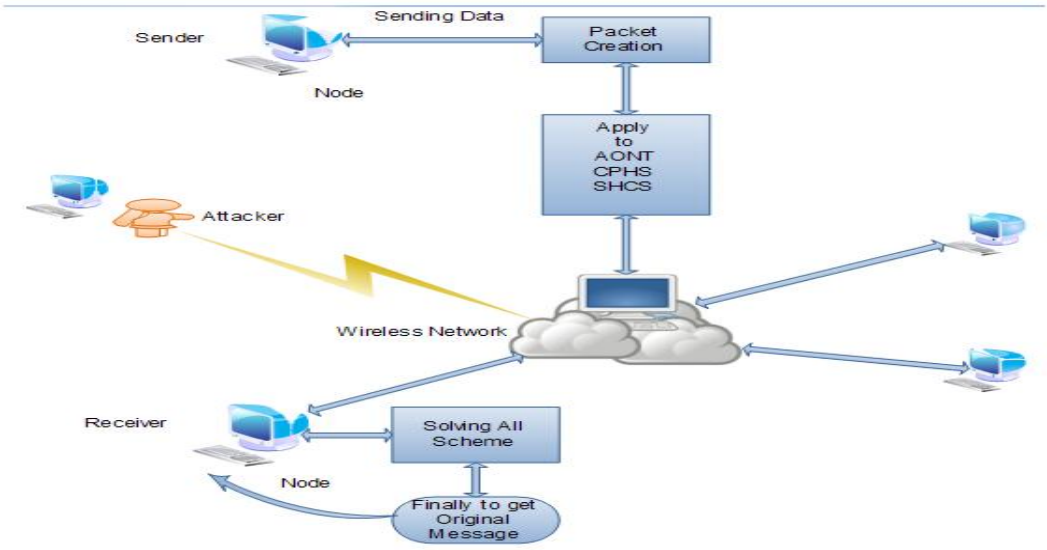
The jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address.

An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key.

A strong hiding commitment scheme, which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum

III. SYSTEM ARCHITECTURE

Systems Architecture is a generic discipline to handle objects called "systems", in a way that supports reasoning about the structural properties of these objects. Systems Architecture is a response to the conceptual and practical difficulties of the description and the design of complex systems.To prevent the jamming under an internal threat model, particularly the adversary who is aware of packet hiding and the implementation details of network protocols at any layer in the network stack.Following techniques has been used to ensure whether the correct messages are delivered at the destination .

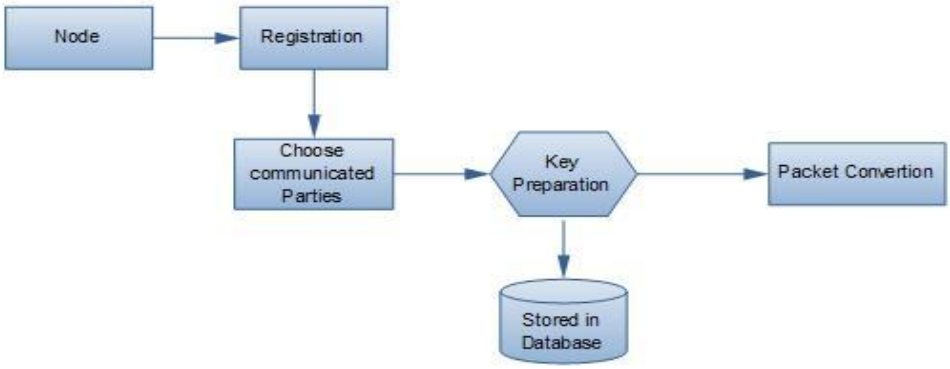


IV. MODULE

- Key Pre processing and Packet Conversion
- AONT Scheme
- SHCS Scheme
- Crypto Puzzles
- Medial node Method (MNM)
- Packet Transmission

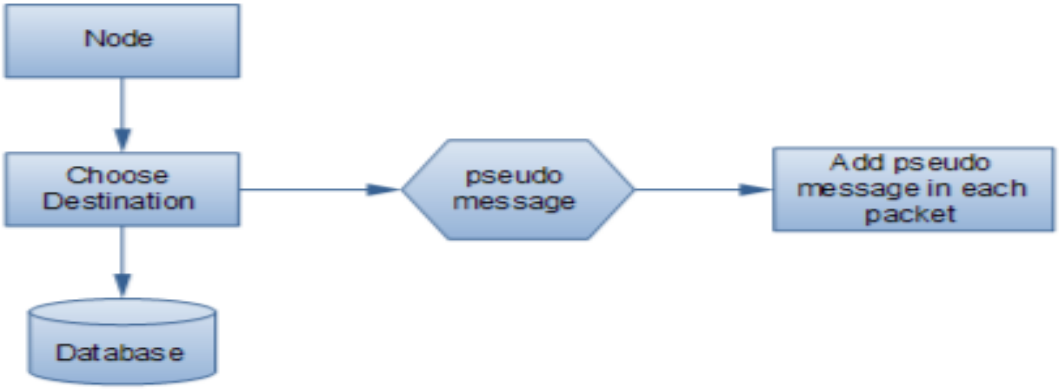
KEY PRE PROCESSING AND PACKET CONVERSION:

Key Processing is a process of pre- distribution of the keys. Each node join in the network the server will provide the symmetric key for set of nodes. In this process the symmetric key algorithm is used for communication. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. After choosing the destination the sender converts the desired transmission packet depending upon the size of the physical layer capacity.



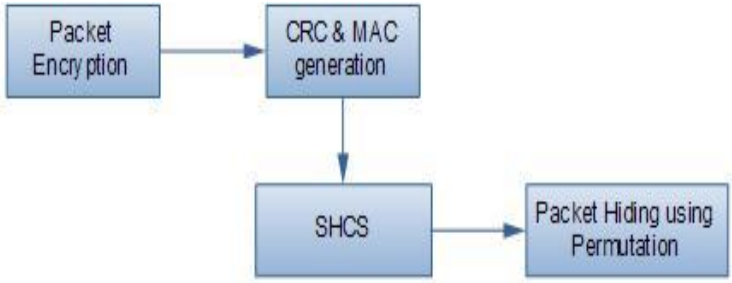
AONT SCHEME:

A CPHS (All-or-Nothing Transformation) is serves as a publicly known and completely invertible preprocessing step to a plaintext before it is passed to an ordinary block encryption algorithm. When a plaintext is preprocessed by an AONT before encryption, all cipher text blocks must be received to obtain any part of the plaintext. Therefore, brute force attacks are slowed down by a factor equal to the number of cipher text blocks, without any change on the size of the secret key.



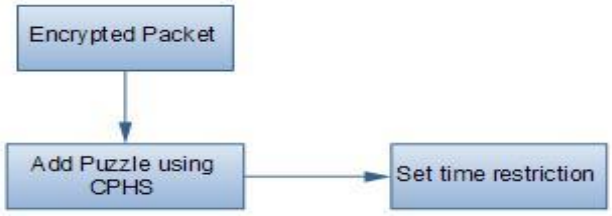
SHCS SCHEME

A strong hiding commitment scheme, which is based on symmetric cryptography. To reduce the overhead of SHCS, the decommitment value d (i.e., the decryption key k) is carried in the same packet as the committed value C. This saves the extra packet header needed for transmitting d individually. To achieve the strong hiding property, a sub layer called the "hiding sub layer" is inserted between the MAC and the PHY layers. This sub layer is responsible for formatting m before it is processed by the PHY layer. In the SHCS scheme padding and permutation are used for security. Because of this scheme each frame contains the source and destination address, CRC value, MAC header details, length of the frame.



CRYPTO PUZZLES

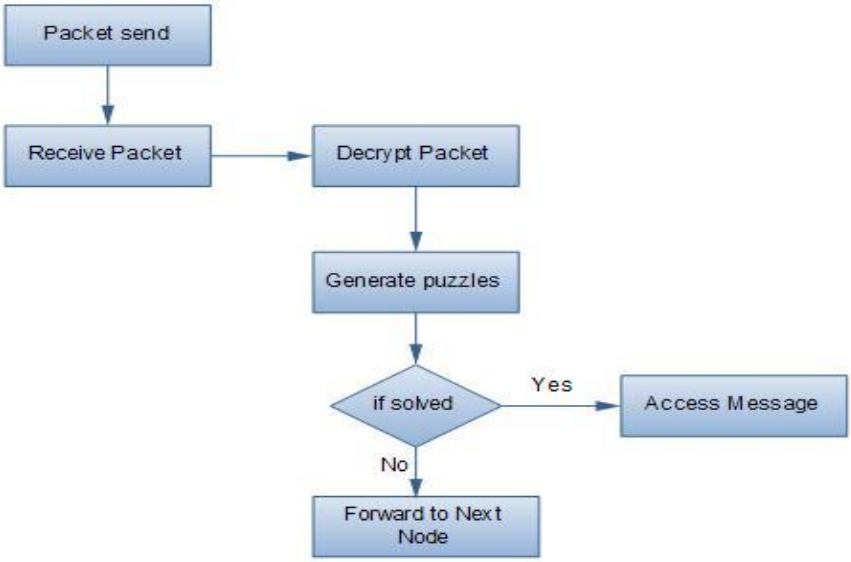
Cryptographic Puzzle Hiding Scheme (CPHS) is technique which is used to provide the security in non-secure channel. A construction called time-lock puzzles, which is based on the iterative application of a precisely controlled number of modulo operations in this process the sender generate the puzzle for packets and set the time for solving the puzzles. By using this receiver can decode the packet when all the packets are received. The time-lock puzzles used to reduce the packet accessing of time of attackers.



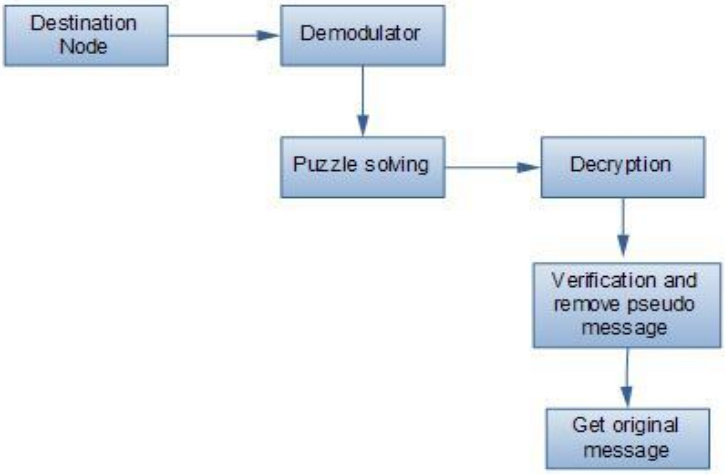
PACKET TRANSMISSION AND RECOVERY

The modulator received the bit stream of the packet and it modulates them into suitable format for transmission. The receiver may be within a communication range the packets send directly to the receiver. Otherwise it sends via multi-hop nodes. The receiver receives and identifies the packets by using the key. After that they demodulate, de-interleave and decode the packet.

PACKET TRANSMISSION



PACKET RECOVERY



V. CONCLUSION

An internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. The jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. It has been evaluated the impact of selective jamming attacks on network protocols such as TCP and routing to show that a selective jammer can significantly impact performance with very low effort. Three schemas had been developed and transform a selective jammer to a random one by preventing real-time packet classification. New technique proposed towards the security of the data by piggyback the data with the sequence ID and with the host name. Along with the piggybacking it also maintains the strong hiding scheme that provides the packet from loss and stored in the buffer. The congestion control is maintained by following the sequential number ID of the packets. In the wireless network, the confidentiality of the data is more important aspect and is maintained in this paper by piggybacking the packets without loss.

FUTURE ENHANCEMENT:

The System evaluated the impact of selective jamming attacks on network protocols such as TCP and routing but in the future work will be concentrating on many other protocols like UDP, ICMP, IGMP, SCTP, PIPE, HIP, SMP, and SMTP.

REFERENCES

[1]. A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.
[2]. A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.
[3]. B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.
[4]. G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.
[5]. G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. Mobile Computing and Communications Review, 7(3):29–30, 2003.
[6]. IEEE.IEEE802.11standard. http://standards.ieee.org/getieee802/ download/802.11-2007.pdf, 2007.
[7]. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.