National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040
Impact Factor: RJIF 5.22
www.nationaljournals.com
Volume 3; Issue 1; January 2018; Page No. 1115-1119

Autonomous encoding of jamming attack by commitment scheme in multi-hop wireless sensor network

Sunil Gupta[1], Vedant Rastogi[2]
[1] CSE, Department of CSE, Alwar, Rajasthan, India
[2] Department of CS&E, I.E.T., Alwar, Rajasthan, India

Abstract
In the field of wireless sensor network, it is a very emerging technology based area of and very popular for research because it is very useful in many areas such as health sector, military application and other commercial application i.e. it addresses the many problems which is not handled by human being easily. Wireless sensor nodes have limited storage capacity and processing signal power to complete their task. Because it is small and cheap, it can be deployed easily in a hostile and unattended environment. There are so many attacks on wireless sensor network, in wireless networks due to its open nature it leaves vulnerable to the intentional interference attacks, called them as jamming. This can be used for mounting Denial-of-Service attacks in wireless network. Typically jamming has been addressed under external threat model in this addressing problem of jamming attacks in wireless network and considering adversaries is active for only short period of time, selectively targeting messages of high importance. For prevention of these attacks we are implementing three schemes that prevent real time packet classification by combining cryptographic primitives with physical layer and also strong hiding commitment schemes and cryptographic puzzle hiding schemes.

Keywords: selective jamming, denial-of-service, packet classification, cipher text, plain text

Introduction

The application of wireless technology becomes very important that brings world together. This is used in every area such as education, agriculture, pharmaceuticals, manufacturing, military and other multidisciplinary area etc. So these fields are connected via wireless communication and they are transmitting data and many times this data may be confidential due to this, it requires security. Generally there are two popular wireless networks as client-server and ad-hoc network. The wireless network depends on availability of wireless medium to connect participating nodes. In this at the time of sending message to receiver there may be eavesdropping in wireless transmission. Cryptographers often make incorrect choices among systems they switch to system that is stronger against serial attacks but is weaker against the best attacks i.e., against parallel attacks. Wireless Sensor Networks (WSN) is an active research area in to days computer science and telecommunication. The development of clustered sensor networks have recently been shown to decrease system delay, save energy while performing data aggregation and increase system throughput. Wireless sensor network may consist of hundreds or thousands of sensor nodes and can spread out as a mass or placed out one by one. The sensor nodes collaborate with each other over a wireless media to establish a sensing network, i.e. a wireless sensor network because of the potentially large scale of the wireless sensor network each individual sensor node must be small and of low cost. The availability of low cost sensor nodes has resulted in the development of many other potential application areas. The sensor network can provide access to information by collecting, processing, analyzing and distributing data from the environment.

1. Types of Cryptography
2. Symmetric Cryptography

The symmetric cryptography used same key for encryption and decryption at sender and receiver side as shown in the figure 1.6. This is also called as dual functionality. In another form symmetric key is also called as secret key because all this process depends on every user to preserve the key secretly. If this key gets in the wrong hands then that person is able to decrypt all the transmitted data which is encrypted by same key. Sender and receiver who want to transmit the data by using symmetric key encryption must contain set of key for further use. If user A and user B want to transmit the data so both the user need same key for encryption and decryption process. If user A want to transmit the data using symmetric encryption to user B and user C then he need different key for each user. This is simple until the users are not increased up to several hundred of user for a long duration of time may be of several months. If users are increased hundreds then it is very difficult to keep the track that which key belongs to which user. If user A wants to transmit the data to 10 other users then user A has to keep the track of all the keys of new user with whom he wants to communicate. So it means user A has to spend his time for looking the right key for right person then he can do the actual work.

Use of Symmetric Method for Encryption and Decryption

- The encryption method is simple in use for every user.
- Each user can use the same encryption algorithm to

transmit the data so no need to develop another algorithm.
- Safety of system is mostly depending in the length of key.
- Used key for symmetric key are quite short.
- This type of key cipher are used to
- High rates of data throughput.
- Symmetric-key ciphers can be used as base to build various cryptographic instruments.
- This ciphers can be used to made stronger ciphers

This encryption is separated in two types as follows

1. Stream cipher symmetric cryptography
2. Block cipher symmetric cryptography

A stream cipher method process the input data constantly element by element up to the end of the entire stream. In another way called as block cipher the input of single block element is process at a time and output is produced, the output is also in the form of block itself. So we normally select the block cipher because it is more efficient and provide more security. Mainly the secret key is belongs to symmetric key cryptography in which the original text is converted into cipher text which can be decoded by the same private key in the original form again. The key used for these operations is similar in encryption and decryption process; if not similar then some transformation is required to get another related key. These keys are used in practical implementation and usually maintain the secrecy of information. Simple concept of symmetric cryptography is presented in diagram 1.7 [6].

Asymmetric Cryptography

Public key cryptography is most important and evolutionary research in the complete history of cryptography. Before this research all cryptographic operation are depend on the substitution and permutation methods and some tools are used for the same type of operation. So most of the cryptographic work is done in a manual way only as practically it was not implemented. But then a major change occurs by the progress of rotor machine which is based on the electromechanical rotor. These rotors are different as per the complexity level. As level increased complexity also increases and it became more difficult to decode the rotor. Public key cryptography offers various fundamental advantages on all the system which are used before the evolution of this system. It uses various mathematical function and processes as compare to conventional system which make use of substitution and permutation. Also public key cryptography has advantage over symmetric encryption as it uses separate key for encryption and decryption process. In previous system they used single and unique key for conversion. Use of multiple keys provides better confidentiality and authentication as compare to previous system. The security of every security system or any algorithm depends on the length of key used and the complexity involved in the encryption process. More complexity means tougher to break the security.

In symmetric key cryptography single and unique key is used between both entities while on the other hand public key cryptography each user used multiple and different keys. But this both the keys are logically related with each other. If one key is used for encryption of message then other key is used to decrypt the same message to get the original data. While in public key system one key is said to be public and other is private. Public key is the key which available to everyone and private key belongs to the owner only. As public key is common between the people so it is present in the directories and email address of the people. So this is easily available to every user to encrypt or decrypt the data when sender and receiver need to communicate. Both public key and private key are logically related but we cannot calculate one from the other. It means if attacker get the public key of one user then there is no relation between the both the keys so another users private key can not be calculated by using the known public key.

A transfer a packet m to B, node J distribute m by receiving only the first few bytes of m. Jamming node J then corrupting m beyond recovery by interfere with its reception at B. we provide and solve the problem of address of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, do not address packet classification methods based on protocol Semantics.

Proposed System

In this paper we are classify problem of jamming attack, proving the advisory knows with network secrets and the details about network protocol implementation in network stack for any layer. The adversary attacks on "High importance" messages using network knowledge. For example the congestion target route-request/route reply messages in routing layer to avoid route discovery in TCP session target the TCP acknowledgement and degrade throughout.

System Architecture

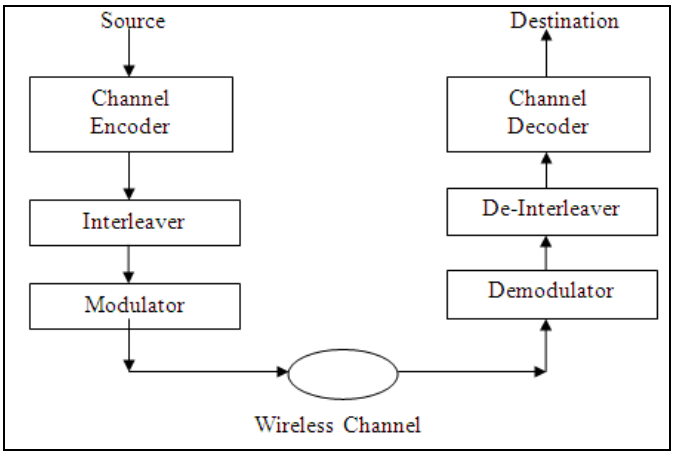

Fig 1: System Architecture

Real, Time Packet Classification

Consider the generic system of communication in PHY layer, a packet m is encoded, interleaved and modulated before it is transmitted over the wireless channel. At receiver side, the signal is demodulated, deinterleaved and decoded to recover original packet m. If the encryption key of hiding scheme Ire to remain secret, the static part of transmitted packet could potentially leads to packet differentiation. This is due to

different efficient method of encryption like block encryption, the encryption with same key for prefix plaintext gives static cipher text prefix. The adversary which is aware with protocol uses static portions of transmitted packet to differentiate it.
At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B.

Selective Jamming Module
In the selective module we will consider the network performance in selective jamming attacks. The implementation is in two multi-hop wireless network scenarios. The first scenarios, the TCP connection established over a multi-hop targeted by attack in wireless route. In second scenario network layer control messages transmitted during route establishment process which targeted by jammer, would be encryption of transmitted packets with static key. In broadcast communication the decryption key must known to all receivers, so they can compromise. Then adversary of decryption key can start decryption when first cipher text block is received.

Hiding Based On Committments
In this module we describe about the problem which is arises in packet classification of mapping to hiding property of the commitment schemes and also proposed schemes based on commitment for packet hiding.

Mapping to Commitment Schemes
Cryptographic primitives gives commitment schemes which allows an entity A, to commit to a value m to an entity V while keeping m hidden. These commitment schemes one formally defined as follows –
Commitment Scheme- This scheme divided in two phase of interactive protocol defined as triple {A,B,C},where Set A={P,V} defines two probable polynomial systems, where, P is committer and V is verifier. Set m denotes space for message and set B{ti, Fi} defines events or conditions happens with protocol steps ti(i=1,2) as per functions fi(i=1,2). On the time of commitment step t1, A use commitment function fi=commit 1 to generate a pair (c, d) =commit (m), where (c, d) is called commitment/de-commitment pair. At the last of stage t1, A gives commitment C to V.

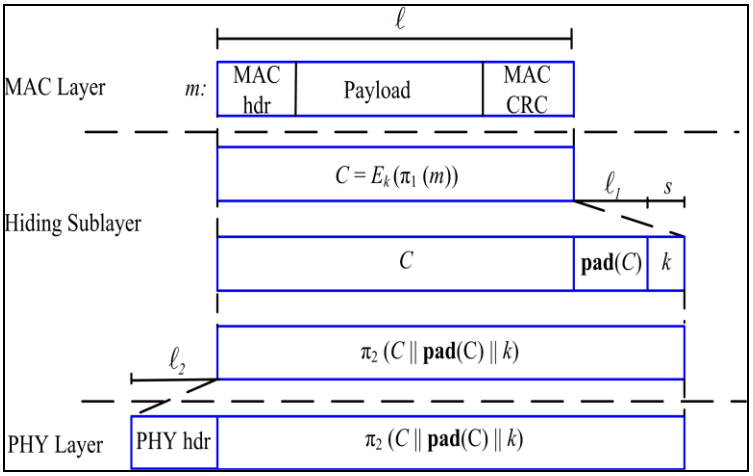

Fig 2: Functions of the Hiding sub Layer

Consider a frame m at the MAC layer delivered to the hiding sub layer. Frame m consists of a MAC header and the payload, followed by the trailer containing the CRC code. Initially, m is permuted by applying a publicly known permutation π1. The purpose of π1 is to randomize the Fig. 4. Processing at the hiding sub layer input to the encryption algorithm and delay the reception of critical packet identifiers such as headers. After the permutation, π1(m) is encrypted using a *random* key k to produce the commitment value C = Ek(π1(m)). Although the random permutation of m and its encryption with a random key k seemingly achieve the same goal (i.e., the randomization of the ciphertext), show that both are necessary to achieve packet hiding. In the next step, a padding function pad() appends pad(C) bits to C, making it a multiple of the symbol size. Finally, C||pad(C)|| k is permuted by applying a publicly known permutation π2. The purpose of π2 is to ensure that the interleaving function applied at the PHY layer does not disperse the bits of k to other symbols. now present the padding and permutation functions in detail.

Padding–This function reduces time and uses few symbols at time of transmission.

Permutation–It is applied on two public permutation that means π1 and π2 at different processing stages. Permutation π1 is used for classification of plaintext blocks. Hence, to reconstruct these fields, all corresponding cipher text blocks must be received and decrypted. Moreover, header information is pushed at the end of π1(m).. For example, consider the transmission of a MAC frame of length 2,336 bytes which carries a TCP data packet. The MAC header is 28 bytes long and has a total of 18 distinct fields. TCP header is

20 bytes long (assuming no optional fields) and has 17 distinct fields. Assume the encryption of a fixed block of 128 bits. Packet π1(m) is partitioned to 146 plaintext blocks {p1, p2,... , p146}, and is encrypted to produce 146 cipher text blocks C = c1||c2||... ||c146. Each field of the TCP and MAC headers is distributed bit-by-bit from the most significant bit (MSB) to the least significant bit (LSB) to each of the plaintext blocks in the reverse block order. This process is depicted in Fig4.3

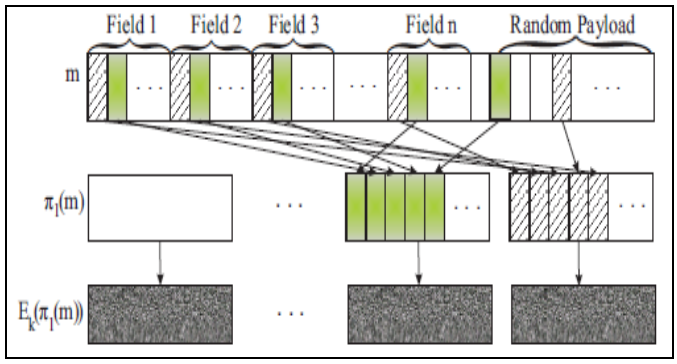

Fig 3: Permutation π1 on Packet m.

For fields longer than one bit, bits are numbered from the LSB to the MSB and are placed in reverse order to each plaintext block.

To recover any field i that is ℓi bits long, the last ℓi cipher text blocks must be received and decrypted. If ℓi > ℓb, where ℓb denotes the cipher text block length, the bit placement process continues in a round robin fashion. The second goal of the permutation π1 is to randomize the plaintext blocks. Assuming a random payload, the permutation distributes the payload bits to all plaintext blocks processed by the encryption function, thus randomizing each cipher text block. Permutation π2 is applied to reverse the effects of interleaving on the bits of k, so that k is contained at the packet trailer. Interleaving can be applied across multiple frequencies on the same symbol (e.g., in OFDM), or it may span multiple symbols. For example, consider a d × β block inter leaver. Without loss of generality, assume that β = q, and let the last n rows of the last block passed via the inter leaver correspond to the encoded version of the random key k. Permutation π2 rearranges the bits of k at the interleave matrix Ad×_ in such a way that all bits of k appear in the last n columns. Therefore, the bits of k will be modulated as the last n symbols of the transmitted packet. Note that this operation affects only the interleave block(s) that carries k. For the rest of the packet, the interleaving function is performed normally, thus preserving the benefits of interleaving. For PHY layer implementations in which interleaving is applied on a per symbol basis (e.g, 802.11a and 802.11g), the application of permutation π2 is not necessary.

System Analysis and Risk Management

Analysis part represents the customer requirements e.g. Analysis step includes stepwise specifications of the program or process to represent requirements, analysis includes three domains

- Information domain
- Functional domain
- Behavioral domain

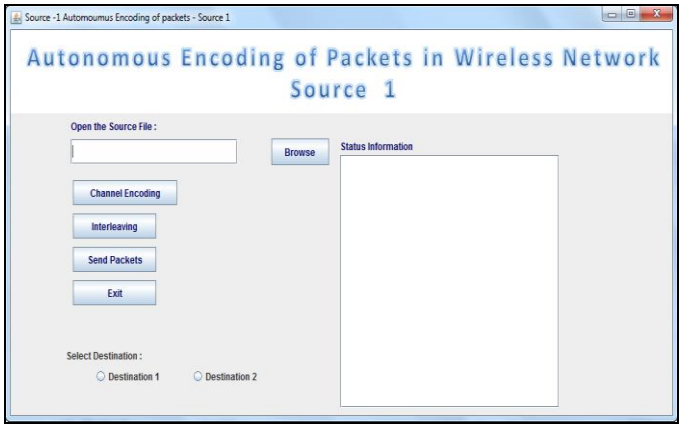

Fig 5: Main Input Form for Source 1

Puzzle Generated

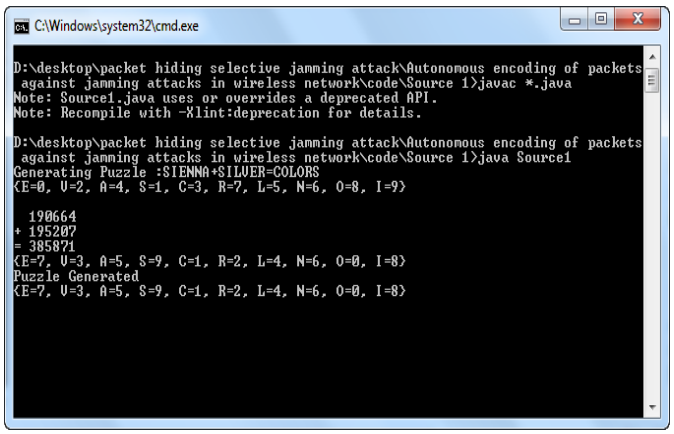

Fig 6

Conclusion

In this paper introduced the attacks in wireless network. In this addressing problem of jamming attacks in wireless network and considering adversaries is active for only short period of time, selectively targeting messages of high importance. They can attacks on TCP and on routing. Selective jamming attacks launched by performing real time packet classification at physical layer. For prevention of these attacks we are implementing three schemes that prevent real time packet classification by combining cryptographic primitives with physical layer and also strong hiding commitment schemes and cryptographic puzzle hiding schemes. The solution is provided for saving the data from an unauthorized person. The different stages of the algorithm provide different techniques and through this stage provide the solution for our problem.

Future Scope

In future, we can implement applications for security problems. In this paper have implemented system for the security using commitment schemes and cryptographic puzzles. So the techniques can be used and implementation can be possible with them. In future the working for security is possible in which provide the security through the schemes like all or nothing transformation. This scheme also provide in physical layer which prevents selective jammer and no possibility to classify packet. It also provide security for TCP

where the high importance messages are targeted.

References

1. Brown TX, James JE, Sethi A. 'Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages, 2006, 120-130.
2. Cagalj M, Capkun S, Hubaux JP. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing. 2007; 6(1):100-114.
3. Chan A, Liu X, Noubir G, Thapa B. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.
4. Liu C, Ichsler H. Evolutionary Pursuit and Its Application to Face Recognition, IEEE Trans. Pattern Analysis and Machine Intelligence. 2000; 22(6):570-582.
5. Dempsey T, Sahin G, Morton Y, Hopper C. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE. 2009; 24(8):23-30.
6. Desmedt Y. Broadcast anti-jamming systems. Computer Networks. 2001; 35(2-3):223-236.
7. Kok-Keong Loo, Tahir Naeem. Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, 2009, 3(1).
8. Jongdeog Lee, Krasimira Kapitanova, Sang H. Son, The Price of Security in Wireless Sensor Networks Computer Networks: The International Journal of Computer and Telecommunications Networking, 2010, 54(17).
9. Jagbir Dhillon, Krishna Prasad, Rajesh Kumar, Ashok Gill. Secure Data in Wireless Sensor Network By Using DES, International Journal of Wireless & Mobile Networks (IJWMN), 2011, 3(3).
10. Prabhudutta Mohanty, Sangram Panigrahi, Nityananda Sarma, Siddhartha Sankar satapathy. Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey, Journal Of Theoretical And Applied Information Technology Jatit, 2005.
11. Ray Hunt. Network Security: The Principles of Threats, Attacks and Intrusions, part1 and part 2, APRICOT, 2004.
12. Abhishek Pandey RC, Tripathi. A Survey on Wireless Sensor Networks Security International Journal of Computer Applications (0975-8887), 2010, 3(2).
13. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary. Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing Yang Xiao.