Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.459 – 465

RESEARCH ARTICLE

Preventing Selective Jamming Attack in Wireless Sensor Network by using Packet Hiding Method

Rahul S Sapkale[1], Mangesh P Khalale[2], Vaibhav S Jagtap[3], Laxman D Nikam[4]

Final Year, Computer Engineering, S.V.I.T. Nashik, Pune University, India

[1] rahul007hr@gmail.com

[2] mangeshkhalale9@gmail.com

[3] jagtapvaibhav85@gmail.com

[4] laxman.nik23@gmail.com

Abstract—In wireless network attacks interferes with set of frequency bands used for communication by transmitting continuous jamming signal or several jamming pulse. This intentional interface with Wireless transmission can be used as Launch pad for mounting denial of service attack on wireless censored networks [1][2].for addressing jamming attack typically used external thread model with half duplex or hull duplex model however ,ignoring these internal execution model well as protocol Specification & network secret can launch low-effort jamming attack which will difficult to detect & counter in these paper we uses a external as we as internal thread model for full duplexing &We show that selective jamming attack can be launch by executing real-time packet classification. Method on PHY layer to make these attack has unpleasant we used real time packet classification. Strong packet hiding commitment scheme as we as using Brute Force algorithm for standard [IEEE 802.11b, 802.11, org 9.0]. We reduce security of our method is undeniable as we as evaluate their computation as well as communication overhead.

Keywords—selective jamming, denial of service, real time packet specification, packet hiding, all-or-nothing

I. INTRODUCTION

Wireless technique is the technique, which is rapidly increasing in our day to day life. It allows the communication between two or more devices, without any physical connectivity such as cabling. we know that it is possible transport mechanism between devices through wireless network. We know that Wireless Network uses transport mechanism to communications takes place between devices. One of fundamental way for degrading the network performance is by jamming wireless transition adversary wireless transition the adversary corrupts transmitted messages by causing electromagnetic interference in network operational frequencies and proximity of receiver [2][3]. We consider a sophisticated adversary model in which the adversary model is gaves implementational details via physical layer and network model.as well as adversary model launches selective jamming attack in which it targets specific “high” range packet in that TCP acknowledgement(Ack). And congession control for the encryption and decryption media for strong commitment scheme for the data decryption regretting original data.

For that we uses adversary modularity, that consist of :-

1)Communication link
2)Interleaving processes
3)Modulating process
On the other hand for receiver side:-
1)De-modulating process.
2)De-interleaving process.
These can be active for short period of time. therefore it expands less magnitude of energy. For performing a our module scenario that uses a MAC layer frame as well as algorithmic commitment scheme consist of,

1)Real time packet classification.
2)Strong Packet Hiding Commitment Scheme.
3)Brute Force Algorithm.
4)Combine Cryptographic Mechanism.
5)Cryptographic Puzzle by using physical layer parameter.

In this paper, we deal with the problem of jamming under an internal threat model. Here the attacker who is aware of networking secret and the implementation detail of all the layers of network protocols ISO/OSI model.

1) **Jamming Attack: -** Attacker interferes with set of frequency bands used for communication by transmitting continuous jamming signal or immunious noise.

Types of Jamming Attack: -
in perhaps Dos attack (Denial of service) recently used jammer attacks are given below,
1) Constant Jammer: - Continuously emits noise, radio signals
2) Deceptive Jammer: - Continuously broadcast fabricated messages or reply old one messages
3) Random Jammer :- alternate between period of continuous jamming and inactivity or uses any one or both Constant, Deceptive jamming or mixing of both attacks
4) Reactive Jammer : - who jams only when transmission activity is detected.

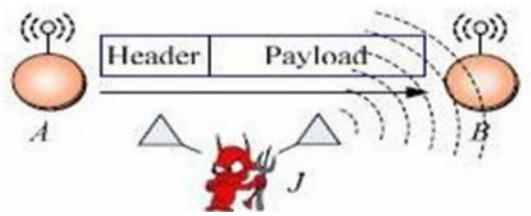

Fig1:Antonyms of a selective jamming attack

2.1) Constant Jammer: -
As name indicates this type of jammer attack is continuously emits noise , a radio signal. Constant jammer can be generated using two types of devices. First type is by using waveform generator , which is continuously emits as well as sends out radio signal which can be emanates a noise, so noise immunity higher whereas transmission takes placed. In second type of jammer which is used the normal wireless sensor network device. In this anther, it will be focused on the second type , which is based on MICA2 Mote platform . These attacks able to deny complete access to the channel by monopolizing the wireless medium. In IEEE 802.11 based on MAC protocols and virtual carrier wireless mote sensing is used at the MAC layer to determine the availability of the wireless media. Jamming attack can be determined at the MAC layer through attacks on the RTS/CTs frames or DATA frames. A significant advantage of MAC layer jamming is that the adversary node consumes less power in targeting these attacks as compared to the physical continious radio signal jamming. Here, we focus on DoS attacks at the MAC layer resulting in collision of RTS/CTS control frames or the DATA frames.

2.2) Deceptive Jammer: - this type of jammer attack is continuously adding regular packets to the channel or continuously transmits massages or old one massage. This can be causing that user will be believe that this massage are true that they are not fabricated this cause communicator gives response to the this massages so that cause this network jammer has jammed this way and data can be corrupted or hacked or stolen happens. for this deny of this attack we can checking node in which we are transmitting packets if continuously incoming packet

stream are detected for time period then we regards this note and select another node which is free also encryption or decryption methods or strong packet hiding method are used for this transmission.

2.3) Random Jammer :- As name indicates this type of jammer attack is randomly attack one by one or alternate between Constant jammer or Deceptive jammer .this can be alter between periods of continuous jamming and inactivity so cause of this this type of jammer sometimes its act like continuous jammer which is , sent continuous radio signal or sending continuously packet or continuously emits noise to jammed the network otherwise its act like the deceptive jammer which is continuously sends out fabricate massages or reply old one massages or continuously adding packet whether has transmitting between two nodes are detected.

2.4) Reactive Jammer :- As above stated three models are responsible for jamming attack whenever in type of active jammer because of they can try to block the channel media directly or indirectly proportional to the observed traffic patterns on the channel media. Active jammers are most often effective because they loading traffic on particular channel as instance of time they keeping channel always on busy condition . For that methods are easy to detect but, an another approach of jamming attack on wireless sensor network communication is to use an reactive jamming strategy. As reactive jammer, it's not necessary that it has working on basis on criteria of this above stated three types of jamming attack constant, deceptive and random however for reactive jammer attack it selects that communication node that there is no one communicating and create jamming attack instance as jam's node .until this jammer stays in sleeping mode but keeping processed that channel in idle state. as soon as when this can detected the transmitting data or radio signal at that instance attacker activate and jam's the network nodes .jammer can be targets the reception of massages, transmission of packets etc. resulting the total packet loss or garbage data invocation or many more resistances on sending media via information is corrupted. because of these reactive type of jammer are very harder to detected on the transmission media.

PROBLEM STATEMENT AND ASSUMPTIONS

Problem Statement:-

Consider the model based scenario depicted in Nodes A and B communicate via a wireless link as wireless sensored network. In between the communication range of both Node A and Node B, there is a jammer Node J. When Node A transmits a packet m to Node B, Node J classifies packet m by receiving only the first few bytes of packet m. Node J then corrupts packet m beyond recovery by interfering with its reception at Node B. We understand the problem of preventing the jamming node from classifying packets m in real time, thus mitigating circumstances of Node J's ability to perform selective jamming. Our goal is to Preventing a selective jamming attack in wireless sensored network to reactive premices of attacker. Note that in the current work, instead of address packet classification methods based on protocol semantics. Packet Frame description as follows

Preamble:- synchronizing sampling process
PHY hdr :- contain length of frame , transmission rate
MAC hdr :- MAC address of frame
Payload :- ARP packet/IP packet
MAC CRC :- MAC address cyclic redundancy check
PHY trailer :- appending synchronization between sender and receiver

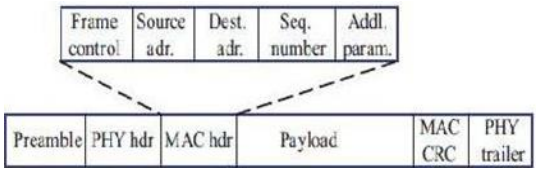

Fig.2 A Standard frame format for a wireless network

System and Adversary Model

Network Model:-

The network consists of a collection of nodes connected via wireless sensored links. Nodes can be communicate directly if they are between communication range, or indirectly via multiple Nodes. Nodes can be communicate with both in unicasting mode and broadcasting mode. Communications can be either without encrypted or with encrypted. For encrypted broadcasting communications, symmetric keys based on RSA algorithm and brute-

force algorithm are provided among all enwrapped receivers. These keys are established using pre provided pairwise keys or asymmetric cryptography.

Communication Model :-

Packets are transmitted at a rate of R bauds bits/sec. Each physical layer symbol accompanying to q bits, where value of q bits is defined by basic digital modulation scheme. Each and every symbol carried q data bits, where $\frac{\alpha}{\beta}$= is the rate of the physical layer encoder. Here, transmission bit rate is equal to qR bits/sec and the information bit rate is qR bits/sec. Spread-spectrum techniques such as frequency hopping spread spectrum (FHSS), or direct sequence spread spectrum (DSSS) may be used at the PHY layer to protect ,transmissions from jamming. Spread-spectrum techniques provides immunity to interference to some extent (from 20 to 30 dB gather), but a powerful jamming attackers is still capable of jamming data packets as randomly or deceptively. Transmitted packets have the standared format depicted in Fig. The preamble is used for synchronization of the sampling process at the receiver. The Physical-layer header contains information regarding the length of the frame, and the transmission rate of packet at network layer. The MAC header determines the MAC protocol version, the destination and source addresses, sequence numbers,payload physical header plus some additional fields. The header of MAC is followed by the frame body that typically contains an ARP packet or an Internet Protocol (IP) datagram. Ultimately, the MAC frame is secured by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer may be appended for synchronizing the sender and receiver.[1][2][3]

Adversary Model:-

We assume the adversary is in control of the communication medium and can jammed messages at any part of the network of his depository (likewise the Dolev-Yao model). The adversary can be operate in full-duplex mode as internal thread model , thus it canbe able to receive and transmit simultaneously. This can be experimented as given, for example, with the use of multi radio transceivers. In addition, the adversary is assembled with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another (likewise contant noise emmiting jammer). For analysis purposes, we assume that the adversary can proactively jammed a number of bits just below the ECC capability early in the transmission. He can then decide to unrecoverable corrupt a transmitted packet by jamming the last symbol.

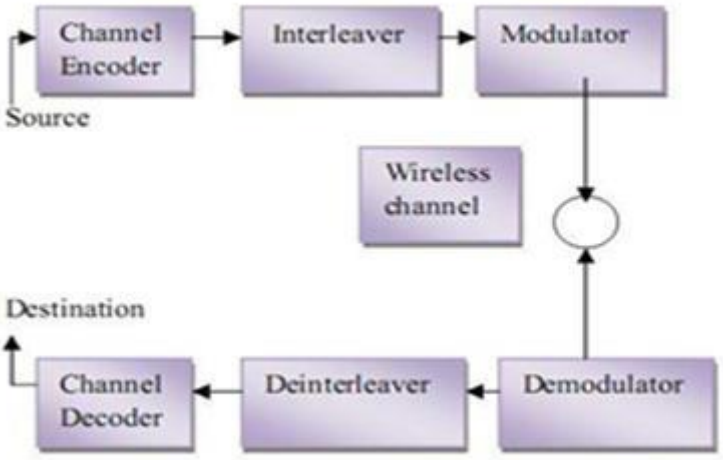

Fig.3 System architecture

In actuality, it has been display that selective jamming can be achieved with far less resources .A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. Although, our model cathches a more potent adversary that can be effective even at high transmission speeds. The adversary is supposed to be calculationally and storage bounded, although he can be far senior to normal nodes. In specific, he can be issue with special Purpose hardware for performing cryptanalysis or any other necessary computation. Solving known hard cryptographic issues is assumed to be long-delayed. For the purposes of analysis, given a cipher text, the most suitable method for deriving the equivalent plaintext is considered to be an compleate search on the key space. The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic for network architectures such as mobile ad hoc, mesh, cognitive radio, and wireless sensor networks (WSNs), where network devices may operate unattended, thus being susceptible to physical compromise.[3]

RELATED WORK:-

In this section, we illustrate the impact of selective jamming attacks on the network performance. We used OPNET Modeler to implement selective jamming attacks in two multi motes wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi motes wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process. In this experiment, we set up a file transfer file between two users A and B connected via a wireless link route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/CTS mechanism was enabled. The jammer was placed within the proximity of one of the intermediate motes of the TCP connection. Four jamming strategies were considered:

1. Selective jamming of cumulative TCP-ACKs.
2. Selective jamming of RTS/CTS messages.
3. Selective jamming of data packets.
4. Random jamming of any packet.
5. Symmetric encryption algorithm.
6. Brute force attacks against block encryption algorithms. In each of the strategies the targeted packets is jammed. Every symbol carries $\frac{\alpha}{\beta}$ q data bits, Where $\frac{\alpha}{\beta}$ = is the rate of the PHY-layer encoder.[1][2]

Selective Jamming at the Network Model: -

In this scenario, we simulated a multi motes wireless network of 'n' nodes, randomly placed within a square area. The AODV routing protocol was used to discover and establish routing paths Connection requests were initiated between random source/destination pairs. Three jammers were strategically placed to selectively jam no overlapping areas of the network. Types of jamming strategies were considered:

1) Continuous and deceptive jammer
2) Random jammer
3) Reactive jammer

We show the number of connections established, normalized over the number of connections in the absence of the jammers. The fraction of time that the jammer was active during simulation, for each Jamming strategy. We observe that a selective jamming attack against RREQ messages is equally effective to a constant jamming attack. However, selective jamming is several orders of magnitude more efficient as it is illustrated.

Strong Hiding Commitment Scheme (SHCS): -

We propose 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. The proposed SHCS requires the joint consideration of the MAC and PHY layers. To reduce the overhead of SHCS, the DE commitment 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.Let, the frame carrying (C,d) before the encoder has length of(l1+l2+l3+…ln) bits assuming that the rate of encoder is $\frac{\alpha}{\beta}$,the output of encoder will be length = $\beta/_{\alpha}$(l1+l2+l3+…ln) for symbol of transmission include $\frac{\alpha}{\beta}$, the output of encoder will be length =$\beta/_{\alpha}$(l1+l2+l3+…ln). for symbol of transmission including $\frac{\alpha}{\beta}$ q bits of key k must be stated as, l1= $\frac{\alpha}{\beta}$ {q-$((l1 + l2)\frac{\beta}{\alpha})$|Q|)}.[1][2][3]

Cryptographic Puzzle Hiding Scheme (CPHS):-

a sender S have a packet m for transmission. The sender selects a random key k^i {0, 1 i^{σ}}of a desired length. S generates a puzzle P=puzzle(k,tp), where puzzle( ) denotes the puzzle generator function, and t_p denotes the time required for the solution of the puzzle. Parameter t_p is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by Ɲ and measured in computational operations per second. After generating the puzzle P, the sender Broadcasts (C, P), where C = $E_t\left(x1(m)\right)$. At the receiver side, any receiver R solves the received puzzle p' to recover key k' and then computes m'=x^{-1} (D_x (c')) If the decrypted packet m' is meaningful (i.e., is in the proper format, has a valid CRC code, and is within the context of the receiver's communication), the receiver accepts that

m'=m . Else, the receiver discards m' The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest[1][2][3]. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its Security does not rely on the PHY layer parameters. However, its higher computation and communication overhead we consider several puzzle schemes as the basis for CPHS.

Real Time Packet Classification:-

The processing of each individual packet by the hiding sub layer. The incurred processing delay is acceptable, even for real-time applications. The SCHS requires the application of two permutations and one symmetric encryption at the sender, while the inverse operations have to be performed at the receiver. Such operations can be implemented in hardware very efficiently. Symmetric encryption such as AES can be implemented at speeds of tens of Gbps/sec when realized with Application Specific Integrated Circuits (ASICs) or Field Programmable Gate Arrays (FPGAs).These processing speeds are orders of magnitude higher than the transmission speeds of most current wireless technologies, and hence, do not impose a significant delay. Similarly, the AONT-HS performs linear operations on the packet that can be efficiently implemented in hardware. We note that a non-negligible processing delay is incurred by the CPHS. This is due to the cryptographic puzzle that must be solved at the receiver. CPHS should only be added when the symbol size at the PHY layer is too small to support the SHCS and AONT-HS solutions.[2][3][4][5]

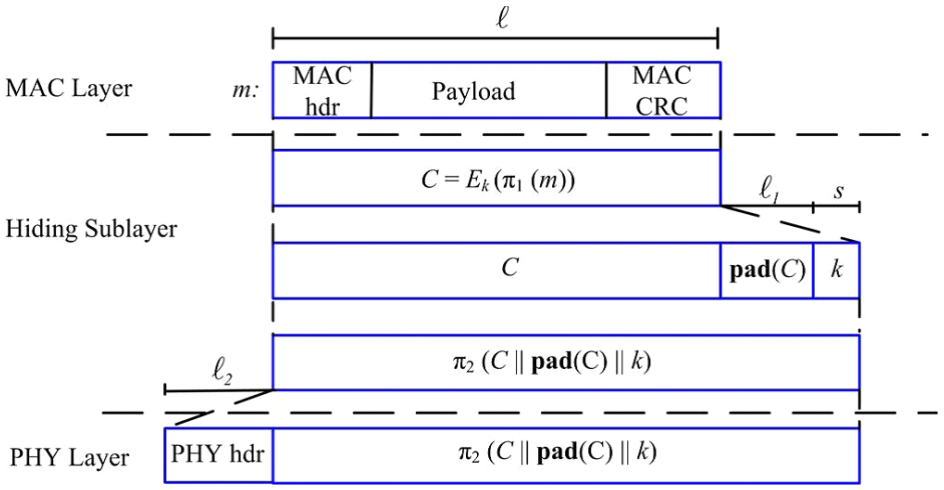

Fig.4 Processing at the hiding sub layer

HIDING BASED ON ALL-OR-NOTHING TRANSFORMATIONS (AONTS) :-

All-or-Nothing Transformations that introduces a modest communication and computation overhead. Such transformations slow down brute force attacks against block encryption algorithms An AONT serves as a publicly known and completely invertible preprocessing step to a plaintext before it is passed to an ordinary block encryption algorithm. A transformation f , mapping message m={ $m_1 \dots \dots \dots m_z$ }to a sequence of pseudo messages $m' = \{m_x \dots \dots m_x\}$, is an AONT if function "F" is a bisection. It is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo messages is unknown and "F'and its inverse F^{-1} are efficiently computable. 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. Several AONT schemes have been proposed that extend the definition of AONT to undeniable security under this model, all plaintexts are equiprobable in the absence of at least one pseudo message. Packets are preprocessed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo messages corresponding to the original packet have been received and the inverse transformation has been applied packet m={ $m_1 \dots \dots \dots m_z$ } is partitioned to a set of x input blocks, which serve as an input to an AONT F{IF}pseudo{IF} Here IF denotes the alphabet of blocks m_1 and x' denotes the number of output pseudo messages with x' 3x .The set of pseudo messages $m' = \{m_x \dots \dots m_x\}$ is transmitted over the wireless medium[2][3][4]. At the receiver, the inverse transformation F^{-1} is applied after

all x' pseudo messages are received, in order to recover m. Linear All-Or-Nothing based matrix scheme shown below for eg.

Let LT= $\begin{bmatrix} l & \cdots & l \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \end{bmatrix}$

According to assumption we can concluded that

Y= $\frac{l}{(n-0-l)}$

According to assumption and result we obtained we can concluded that AONT provides undeniable security.[1][2][3]

CONCLUSION

Jamming attacks on voice communications have been launched since the 1940s in the context of Digital Communications, the jamming problem has been addressed under various threat models.

We present a classification based on the selective nature of the adversary. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine Cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead. We analyze the security of above mentioned schemes and through simulation we can achieve the higher throughput by analyzing the comparative study of these schemes.

References

1) International journal of advanced research in computer & communication engineering volume 2 issues q,September 2013
2) IEEE transaction volume 9 no.1 January /February 2012
3) "selective jamming attack in wireless networks" by Alejandro proano & Loukas Lazos
4) IRACST –International Journal of computer networks & wireless communication (IJCNWC) ISSN;2250-3501,volume 3 No 2 April 2013
5) IOSR Journal of computer Engineering(IORJCE) ISSN;2278-0661,ISBV;2278-8727 Volume-5 issues 3 (sep-oct 2012) pp 13-20 www.iosrjournals.org

