International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

A Survey on Defending Against Jamming Attacks in Sensor Networks

Ms. Archana Patil
Department of Computer Engineering
SKNCOE
Pune,India

Prof. S. P. Pingat
Department of Computer Engineering
SKNCOE
Pune,India

***Abstract*—Sensor Networks are serious security threat called jamming. This actually interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. This paper studies the problem of jamming under an internal threat model, where the attacker who is known of all the network tecniuqe and the details of implementation Technique which results in the difficulty of detection. Jamming Attack is broken down in to layers and the study focuses on jamming at the Transport/Network layer. Here we have done a study on different schemes and Techniuqe that prevent the attacker from attacking the packets.**

Keywords— Jamming, DOS attacks, Wireless sensor Networks

I. INTRODUCTION

Wireless technologies have become most popular in our everyday business and personal Day to Day life. It can be Access one or more devices to communicate without physical connections Does not requiring network or peripheral cabling. As For our knowledge wireless networks serve as the transport mechanism between devices and among devices. Thats because of this wireless open nature these are prone to multiple security threats in which one of the major serious security threat is jamming. Jamming can be interfareing wireless communication and can occur either unfortunatelly in the form of noise or Distrubance at the receiver side. Jamming attacks can be Detect as a special case of Denial of service (DOS) attacks [1]. In simplest form of jamming, the attacker Disturbing with the set of frequency bands used for communication by transmitting a continuous jamming signal [2] or several short jamming pulses [3].

Normally, jamming attacks have been consider under an external threat model, in which the jammer is not part of the network. This is the Physical Device To Avoiding The jamming Attack Under this model, In jamming Technique Sending the continuous or random transfer of high-power interference signals [2] [4]. This type of Technique has several disadvantages. Firstly the Hacker has to store large amount of energy in order to jam the specific frequency . such type of Attck can be easilly detect beacuse of the continues uses of high Distrubance signal .[3], [4], [6].

Another well known Technique against this type of jamming attacks are spread spectrum techniques such jamming is referred as jamming gain. In targeted system, it may jam particular nodes of the system , flows or links, In frequency hopping Techniuqe, direct sequence spread spectrum and chirp spread spectrum [5].thats Aspect of these All technique one thing is same that they working on one special secret code that are use the sender and Reciver.

In this paper, we deal with the problem of jamming under an internal threat model. Here the attacker who is All known about of network Technique and secrets and the implementation details of all the layers of network protocols in the network stack.

II. RELATED WORK

The jamming problems has be occurs in various theting models. The effect of external selective jammer targeting no of various control packet at the MAC layer is studied in paper [7] by Thuente. This Attack is purely based on protocol basis,where they are cosidered No of packet identifiers for encrypted packets such size of packet,time information and sensing of signal of Various protocols. Uniqueness of this packet is minimum length and inter packet timeing is used in order to preventing the selction of signal.

In [8], attempts to use of this protocol at various layer to get three advantages: targeted jamming,jamming gain and probability of reduced Detection. Increase in the effectiveness form utiliazation the feature sufferer/Victim network relative to continuous. In this time the Attacker should be interested in specific parts of the network and Attacking those part this can be lead to jamming gains. As the Reduced probability of detection, the Attacking system network dont know about jamming effect of Attacking.

Selective jamming attacks have been Actually implemented using software defined radio engines [9]. USRP2-based jamming platform called RFReact was implemented by Wilhelm [9] that enables selective and reactive jamming. We develop three schemes that prevent jamming attacks; they are Strong Hiding Commitment Scheme, Cryptographic Puzzle Hiding Scheme and All or Nothing Transformation.

In Strong Hiding Commitment Technique we are use DES[10] algorithm to encrypting the packets where in this technique one secret key is used between client and server. The main Disadvantage is, the Hacker can normally Access the packet by using the brute force attacks so we can

providing the highest security for the packets. In Cryptographic puzzle Hiding Scheme, where every packet is Attached with puzzle and then this packet is encrypted. this puzzle has some time limit to solve this puzzle if this is not solved this packet is dropping and also dealy in receiving the packets. In All or Nothing Transformation, before trasfer the packet this information is in the form of matrix . the jammer can be tried as brute force attack to capture the information in packets.

III. PROPOSED SYSTEM

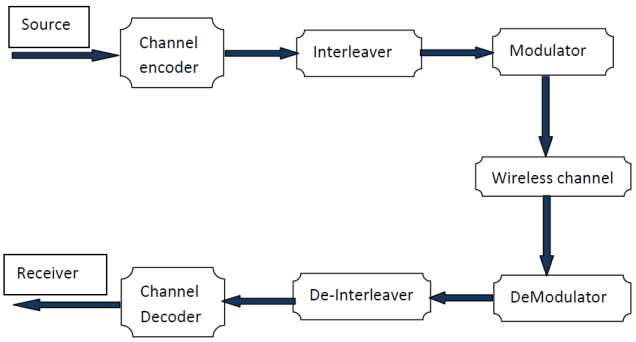

Figure 1: System architecture for packet hiding methods

This technique gives all about the overview of packet hiding to void selective jamming in WNS. At the level of physical layer, packet from the source is encoded,this packet is interleaved and this packet is modulated before the trasfer over the wireless medium. the at reciver , this information is ,demodulated ,de-interleaved and then this information is decoded to obtain the original information of packet. the channel encoder is added extra bits in packet to make this transmission is more robust and to protect against the channel errors. interleaving block takes a sequence of symbol and arranges in different order to protect from burst errors,where as modulator modulates these symbol into waveform for transmission of these packets over the wireless channel.
to obtain the original information ,this packet is passes to th edemodulator where it extracts the original inforamtion bearing signal from a modulated wave.The deinterleaver block arranges the interleaved data in to original format and deinterleaved bits are passed through the decoder. the channel decoder converts the encoded information in to original sequence and then the packets are passed to the Reciver.

A) Strong Hiding Commitment Scheme (SHCS):

This technique is based on asymmetric cryptography. The main goal of is to performing the strong hiding property by keeping by keeping the computation overhead is 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 two properties:

- **Binding:** Deliver the committed value to the receiver, here the sender cannot alter the value once it is committed
- **Hiding:** The reciver can not see the the message if they have get the key,after the key is reciving the key it can show the data.receiver verifies that it is indeed the message to which the sender is committed. Here the role of the committer is implicated by the transmitting node or the sender, 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 R. First, before transmission S constructs

(C,d) = commit (m) C= Ek (1(m)) and d=k

Where Ek the commitment function is an asymmetric Consider that sender S has a packet m for the transmission for R. First, before transmission S constructs

$$(C,d) = \text{commit } (m)\ C= E_k\ (\ _1(m)) \text{ and } d=k$$

Where E_k the commitment function is an asymmetric encryption algorithm (eg. DSA or RSA [11]), $_1$ is a publicly known permutation and k is a randomly selected key. At the receiver side, upon receiving d

the receiver R computes m =	$_1^{-1}(D_k\ (C))$, where $_1^{-1}$
is the inverse permutation of	$_1$ and also it verifies

the signature which is attached to the packets. For reducing the overhead of SHCS, value d called decommitment value i.e. decryption key k which is carried in the same packet with the committed value c. This reduces the burden of carrying the extra packet header which is needed for transmitting d.

B) Cryptographic Puzzle Hiding Scheme (CPHS):

The main idea behind this scheme is to solve for the puzzle at the receiver side by executing a pre defined set of computations before the receiver decrypt the information. The time required for solving the puzzle to obtain the solution depends on the ability of the solver and its hardness. Here the main advantage of this technique is security does not depend on physical layer parameters.
Sender S have a block of packets $m_1,m_2.. m_n$ for transmission purpose. The sender selects a symmetric key k of some length, then S generates a puzzle P = puzzle (k, t_p), where t_p is the time required for obtaining the solution of the puzzle and it is measured in units of time, and puzzle() specifies the puzzle generator function. After generating the puzzle P, the sender attaches the puzzle for block of packets and sends (C,P) where C= E_k ($_1$(m)). At the receiver side, the receiver solves the received puzzle P' and then computes m' = $_1^{-1}(D_{k'}$ (C')). We can also send the same data to 'N' number of receivers with the same attached puzzle. If m' is meaningful the receiver accepts the message or it discards m'.

IV. CONCLUSION

In this paper we discussed about Sensor Networks technique and its problem. We also addressed the problem of selective jamming attacks under an internal threat model, where the hacker is a part of the network who is aware of network secrets and also the implementation details. In order to overcome these kinds of attacks we analyze different technique that combine cryptographic primitives such as strong hiding commitment scheme, cryptographic puzzle hiding scheme and all or nothing transformations. 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. A.D. Wood and J.A.Stankovic, "Denial of Service in Sensor networks",computer, vol.35, no.10, pp. 54-62,2002
2. M.K.Simon, J.K.Omura, R.A.Scholtz, and B.K.Levitt, "Spread Spectrum Communications Handbook," McGraw-Hill, 2001
3. G.Noubir, and G.Lin,"Low Power DOS Attacks in Data Wireless LANs and Countermeasures," in proc.ACM MobiHoc, 2003
4. W.Xu, W.Trappe,Y.zhang and T.wood. The feasibility of launching and detecting jamming attacks in wireless networks. In proceedings of MobiHoc,pages 46-57, 2005
5. R.A.Poisel.Modern Communications Jamming principles and techniques. Artech House Publishers,2006
6. W.Xu, W.Trappe,Y.Zhang and T.Wood. Channel surfing and spatial retreats defense against wireless denial of service. In proceedings of the 3rd ACM workshop on wireless security, pages 80-89,2004
7. 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.
8. 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
9. M.Wilhelm, I.Martinovic, J.Schmitt and V.Lenders. Reactive jamming in wireless networks: How realistic is the threat? In proceedings of WiSec,2011.
10. D.Stinson. Cryptography:theory and practice.CRC press,2006
11. Ravneet Kaur and Amandeep Kaur. Digital Signature, in International Conference on Computing Sciences, 2011