ISSN:0975-9646

A Novel method for securing packets against Reactive Jammer

G.Neelima
Assistant Professor
Dept. of Computer Science & Engineering
Acharya Nagarjuna University

Dr. I. Ramesh Babu
Professor
Dept. of Computer Science & Engineering
Acharya Nagarjuna University

Abstract-The most promising rapid advancements and the distinct features of MANETs resulted into its predominant usage. With its increased usage, intentional inference attacks referred to as jamming attacks are also being increased mainly due to its open nature. Jammers are of many types of which Reactive Jammer is the most malicious one. Reactive jammer initiates jamming activity only when it senses any transmission on a certain channel in the adhoc networks. As a result, a reactive jammer targets on compromising the reception of a message. It can interrupt the transmission of both small and large sized packets. Since reactive type of jammer does not constantly monitor the network, it is less energy efficient than the other types of jammers. These types of jammers can cause massive damage to the communication system by corrupting the data that is being sent which eventually leads to jam in the network. We have addressed the problem by adopting an effective hiding scheme. Our hiding mechanism is the combination of a commitment scheme, a cryptographic puzzle and an authentication mechanism. Commitment scheme is used to generate cipher text along with a committed value. A cryptographic puzzle is chosen to hide the committed value and authentication of the receiver is verified to send the hidden committed value. We analyze the security of our method and evaluate their computational and communication overhead.

Keywords- Jamming attack, Commitment Scheme, Cryptographic Puzzle, Authentication Mechanism

I. INTRODUCTION

The wireless MANET presents a larger security problem than conventional wired and wireless networks. There are different types of attacks in MANETs which challenge their security .One such attack is Denial-Of-Service attack. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent legitimate users of a service from using the desired and required resources and attempts to “flood” a network, thereby preventing legitimate network traffic[6]. The prevention of authorized access to resources or the delaying of time critical operations is the major problem created by DoS attack to Manets. One of the category of DoS attack is Jamming Attack [2]. Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. Jamming attacks also prevents the reception of legitimate packets which exhausts the network resources. Network resources may be Computing Power, Bandwidth and Energy[7] .These attacks operate up on Physical layer and Data Link Layers. Since Jamming attack is a dangerous attack much research is being carried out to identify the malicious node and to mitigate the problems caused by it. Jammer is the node which performs Jamming attacks by obstructing the legal transmission. Jammer categorization is done depending up on the malicious activities performed by it.

In this paper we want to address the problem that is caused by the Reactive Jammer. It gets activated whenever it senses any communication on the channel. If the channel is idle, it remains passive but keeps on sensing the channel. On sensing the transmission, it transmits enough noise resulting some sufficient number of bits which can corrupt the bits in the legitimate packet so that packet checksum is not recovered by the receiver thus leaving the packet discarded by the receiver. Generally to perform jamming attack the malicious node or the intruder must be able to implement “ Analyze and Jam “ technique before the completion of data transmission in the wireless network. Such technique can be implemented either by categorizing transmitted packets using protocol semantics or by decrypting the packets. In the second method the jammer can decrypt the first few bits of the packet to collect the information about the Packet Source, Packet Type and Packet Destination.

After this type of analysis done by the malicious node it can embed sufficient number of bit errors into the packet .If this happens the intended receiver cannot accept the data as it assumes the packet as malicious one. So the Jammer succeeds in making the receiver not to accept its intended packet. To actualize such type of attack extensive knowledge regarding the Physical Layer’s Primitives as well the Specifics of Upper Layers is needed by the jammer.

In addition to that, Jammer should have intimate information about the cryptographic techniques that were used to encrypt the data and also the protocols of the network. In our paper in section 2 we want to focus on the adversaries of jamming attacks and in section 3 up on how the jammer analyze the packets and in section 4 we implement methods for packet hiding against Reactive Jammer and in section 5 we conclude.

II DISTRACTION CREATED BY ADVERSARY IN THE WIRELESS NETWORK

Reactive Jammer always listens to an ongoing activity in the channel. On the detection of legitimate transmission that is being carried out in the channel it immediately sends out a random signal to distract the actual communication between the communicating nodes. This type of attack poses a critical threat to Manets. The malicious node which is performing Reactive jamming can disrupt the message delivery of its neighbouring sensor nodes with strong interference signals. The legitimate packets that are intended to reach the destination will be accepted by the adversary and then they are classified. With the learnt information about the packet and the details of receiving nodes the Jammer can gain control over the network .Then the malicious node can jam messages at any part of the Mobile Adhoc Network.

III Packet Analysis By The Jammer

Consider two nodes S and R in the Mobile Adhoc Network that are communicating via a wireless link. Within the communication range of both the nodes there is a malicious node J whose intention is to jam. When S sends a packet to R, J captures m and analyses it by receiving the first few bytes of m. J then corrupts m beyond recovery by inducing bit errors into the packet .Node R denies to accept the message m as the CRC check was unsuccessful .So from the n packets that were sent only q will be successfully delivered to the receiver R. The intensity of Jammer is measured by PDR.

PDR is given by ∑ Number of packet received / ∑ Number of packet send

To perform this type of jamming Jammer should have control of the communication medium so that it can jam messages at any part of the network of its choice. Jamming can be done by the malicious node with very less number of resources. A Jammer which is well equipped with a single half-duplex transceiver is sufficient to analyze and jam the transmitted packets[10]. The jammer may chose to perform cryptanalysis on the packets in order to know the details of Source, Type of the packet and Destination.

Cryptanalysis is generally chosen as solving crypt arithmetic problems takes much time. For example, consider the transmission of a TCP-SYN packet used for establishing a TCP connection at the transport layer. Assume an 802.11a PHY layer with a transmission rate of 6 Mbps. At the PHY layer, a 40- bit header and a 6-bit tail are appended to the MAC packet carrying the TCP-SYN packet. At the next stage, the 1/2- rate convolution encoder maps the packet to a sequence of 1,180 bits. In turn, the output of the encoder is split into 25 blocks of 48 bits each and interleaved on a per-symbol basis. Finally, each of the blocks is modulated as an OFDM symbol for transmission[5].The information contained in each of the 25 OFDM symbols is as follows:

-Symbols 1-2 contain the PHY-layer header and the first byte of the MAC header. The PHY header reveals the length of the packet, the transmission rate, and synchronization information. The first byte of the MAC header reveals the protocol version and the type and subtype of the MAC frame (e.g., DATA, ACK).

-Symbols 3-10 consist of the source and destination MAC addresses, and the length of the IP packet header.

-Symbols 11-17 contain the source and destination IP addresses, the size of the TCP datagram carried by the IP packet, and other IP layer information. The first two bytes of the TCP datagram reveal the source port.

-Symbols 18-23 contain the TCP destination port, sequence number, acknowledgment number, TCP flags, window size, and the header checksum.

-Symbols 24-25 contain the MAC CRC code.

A packet can be analyzed at different layers and in various ways[10]. MAC layer analysis is achieved by receiving the first 10 symbols. IP layer analysis is achieved by receiving symbols 10 and 11, while TCP layer can be analyzed with the symbols between 12-19. Our example illustrates that with the knowledge of given symbols used by physical layer , the necessary information to corrupt the packet at the reception of intended receiver can be gained by the jammer .In order to prevent that it is very essential for the sender to strongly encrypt the packets .If cryptographic techniques like Public key cryptography is adopted the intended receivers need to be provided with the private key .If Jammer gains that private key then it can easily classify the packets in every transmission.

If it is with Private key cryptography, only one key is used to encrypt and decrypt the data and if the knowledge of that single key is gained by the Jammer then it can analyze the messages throughout the transmission[8]. Block chaining modes like cipher block chaining and cipher feedback mode can be used to encrypt the long messages.

Of self-synchronizing ciphers like Block cipher techniques if part of the cipher text is lost (due to disruption by malicious node), then receiver will lose only some part of the original message (garbled content), and should be able to continue correct decryption after processing some amount of input data. But still Packet Classification by the Jammer is possible thus making the network vulnerable to Denial Of Service attack[2].

IV Proposed Method For Packet Hiding

Reactive Jammer continuously tries to classify the packets that are sent on the network. So a good security mechanism is to be implemented by applying several cryptographic techniques up on the data that is to be transmitted. Strongly encrypted data is very less vulnerable to any type of attack [8]. Even Reactive Jammer also fails to classify the encrypted data if the adopted security mechanism is strong enough.

Reactive jammer starts jamming only when it observes a network activity occurs on a certain channel. As a result, a reactive jammer targets on compromising the reception of a message. It can disrupt both small and large sized packets. Since it has to constantly monitor the network, reactive jammer is less energy efficient than random jammer. However, it is much more difficult to detect a reactive jammer than a proactive jammer because the packet delivery ratio (PDR) cannot be determined accurately in practice. As in Fig 1 Reactive jammers can be of two types. One is Reactive RTS/CTS jammer and the other is Reactive DATA/ACK jammer[4]. We are going to address the issues that arise when the jamming attacks are performed by Reactive DATA/ACK jammer.

For every polynomial time sender is interacting with the receiver ,there is no polynomially efficient algorithm that would allow the receiver to associate c with m and c’ with m’ without the knowledge of d value .For every polynomial-time the sender interacting with the receiver there is no polynomial efficient algorithm that would allow the sender to generate (C,d,d’) such that the receiver accepts the commitments (C,d) and (C,d') with non-negligible probability. As the first step of the commitment scheme sender broadcasts C on to the network after computing (C,d) pair from the message m. when the sender wants to reveal m then the sender releases the decommitment value d, in which case m is known to all the active nodes on the network including the reactive jammer.

In our context, a partial knowledge of m while d is being transmitted can lead to the modification of bits in the packet or the reactive jammer can get the knowledge of destination node's address which may allow it to alter the bits in transmission. To prevent this kind of scenario we introduce an Effective Hiding Scheme. The purpose of this method is to provide high level of security to the data when it is being transmitted on the network. If the data is sent in the encrypted form, the malicious node which may be a reactive jammer cannot read the data. If a node other than the sender possess the shared key that node can act as a malicious node. In order to resist the malicious node from gaining control over the key, security is provided even to the shared key. When the text is transmitted in secret in encrypted form and the key is secured with the help of cryptographic puzzle then the transmission would be a secured one.

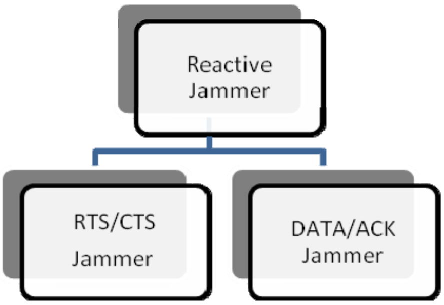

Fig 1 . Categorization of Reactive Jammer

A. Effective Hiding Scheme

As shown in fig 2 we propose a powerful hiding commitment scheme which is based on symmetric cryptography. Our main goal is to implement a strong hiding technique while keeping the computation and communication overhead to a minimum. The proposed scheme consists of a commitment scheme, a cryptographic puzzle and an authentication mechanism.

1) Commitment Scheme

Commitment schemes are one of the cryptographic primitives that allow the sender S to commit to a value d, to the receiver R while making the value of d secure. These schemes are designed so that the node cannot change the value or statement after they have committed to it.Suppose the sender has a packet m for the receiver. As the first step A generates (C, d) = commit(m) where

$C= (E_{K\,(}\; PF(m))$ and d is assigned the value of key k

Here we have chosen an off-the-shelf symmetric encryption algorithm AES as the commitment function. AES is a strong encryption algorithm which is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware[6]. K is a randomly selected key of desired key length. PF is a permutation function. The receiver after accepting the packet computes inverse permutation using IPF and decryption technique.

$M = (\; D_k (IPF(C))$

As per the permutation function that was adopted, bits are numbered from LSB to MSB and are placed in reverse order to each plain text block. Randomization of plaintext blocks is also done. Suppose there is a random payload, PF distributes the payload bits to all plaintext blocks that will be processed by the random function. Interleaving is also applied across multiple frequencies on the same symbol or it may span multiple symbols. In our Hiding Scheme after implementing commitment scheme we have chosen a cryptographic puzzle to operate up on.

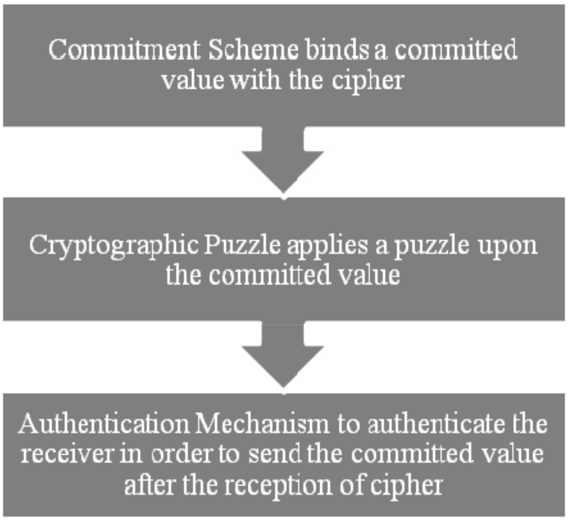
Commitment Scheme binds a committed value with the cipher
Cryptographic Puzzle applies a puzzle upon the committed value
Authentication Mechanism to authenticate the receiver in order to send the committed value after the reception of cipher

Fig 2. Proposed methodology of EHS

2) Cryptographic Puzzle

Our scheme uses cryptographic puzzle which is one of the cryptographic primitives along with a commitment scheme. We have selected an encryption function E_k. When the sender is ready to transmit the data the binded encryption function of the sender selects a random key K of desired length. After the packet m is encrypted with the selected key, cipher text C is generated.

The key K is to be secured using a cryptographic puzzle and then it is to be sent to the receiver. By using cryptographic puzzle technique it would be hard for the reactive jammer to encrypt the cipher [9]. A puzzle that is binded to T seconds is used to hide the key K. The reason for this is if the puzzle is computational and time bounded then the reactive jammer will be unable to solve the puzzle before the transmission of the cipher. Rivest et al .proposed a construction called time lock puzzles which is based on iterative application of a precisely controlled number of modulo operations[8] .

The steps of the puzzle that we have chosen to apply on the key used in our commitment scheme are

- Generate a composite modulus v = xy Where x and y are large random prime numbers.
- Compute t= NT where N is the number of squaring modulo v
- Pick a random number r such that $1 < r < v$ and encrypt d (d=k) like
  $P(d) = d + b^t \pmod{v}$ (where $b=a^2$)

It is to be noted that P(d) can be computed efficiently if $\phi(v) = (x-1)(y-1)$ or the factorization of v are known else without which the puzzle generator has to perform all t squarings to recover d. The output of this puzzle will be (v,a,t,C,P(d)) where C is the encrypted form of plain text and P(d) is the encrypted key with cryptographic puzzle.

3) *Authentication Mechanism*

Authentication is an absolutely essential element of a typical security model. It is the process of confirmation of identity of a user. In our hiding scheme also, we prefer to authenticate the receiver to send the committed value. First the sender node transmits the encrypted form of the text to the receiver. Later it wants to authenticate the receiver to send the key that is needed to decrypt the cipher which was already transmitted. So we propose to implement an authentication mechanism to check whether it is the intended receiver or the jammer which is in the session. As shown in fig 3 the sender sends a nonce word n1 to the receiver along with the Cipher C.

The receiver has to apply an agreed off-shelf hash function up on the nonce and generate the resultant value to the sender. Then it checks and validates the authentication of the receiver. By the completion of this step the sender will come into an agreement with the receiver for the transmission of commitment value P(d) up on which cryptographic puzzle was applied . So we are trying to make our hiding scheme more effective by using the technique of authentication .Reactive jammer may sense the nonce too.

But as the reactive jammer is unaware of the agreed Hash Function it cannot send the hash value of nonce word. If a delay is sensed in sending the hash value of nonce to the sender, alert may be sent to the nodes to implement the jammer mitigation techniques. By receiving the hashed nonce word the sender authenticates the receiver and completes the task by sending the committed value that is needed for encryption.

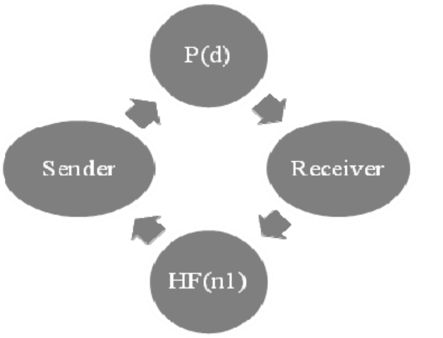

Fig 3 Authentication Mechanism used in EHS

4) *Security analysis of EHS*

For analyzing the security and throughput we have setup a single file transfer between client and server via a multi-hop route using NS2 . Sender has initiated a file transfer of 2 MB to the receiver up on its request. As shown in fig 4a and fig 4b we evaluated the effects of packet hiding using our hiding methodology by computing the Packet Delivery Ratio and throughput .With the adopted hiding mechanism security was high and with no increase in its computation overhead it does not have any impact up on the through put.

Reactive jammer senses the network as active when the sender initiates the communication. The adversary tries to modify the data or classify it in order to get the destination's information. To be transmitted data is left on to the network as cipher and the committed value with which the receiver can view the message is hided with a strong puzzle.

The jammer can attempt to classify m by cryptanalyzing cipher text $C = E_k(\pi_1(m))$. This attack is identical to the effort of classifying m with the transmission of C at the SHCS. The selection of a key of adequate length is sufficient to prevent both cipher text-only and codebook attacks. The transmission of d value in the form of puzzle prevents any receiver from recovering k for at least time t after P(d) has been received. The adversary must finish the classification of m before the transmission of the last symbol of P(d). Suppose that a brute force attack has happened on the missing bits of the puzzle ,the computational load of the jammer increases to a great extent.

Communication Cost –The communication cost of the packet M of length n is based up on the size of the length of the key that was chosen in the encryption algorithm and also the padding done by it. The security of time locks depends on the difficulty in factoring v or finding $\phi(v)$ where $\phi()$ denotes the Euler ϕ function.

As the messages are to be in hidden mode only for short span of time, the modulo is chosen to be of small size and it is refreshed for each session.

Computation Overhead – The computation overhead of the adopted commitment scheme is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the information of header is permuted as a trailer and encrypted , all receivers in the vicinity of a sender must receive the complete packet and decrypt it.

And in the chosen puzzle the sender has to apply one permutation on m, perform encryption for one time with private key and one modulo squaring a operation to hide the value of d. The receiver has to perform n number of squaring operations modulo t to recover d on symmetric decryption and apply the inverse permutation.

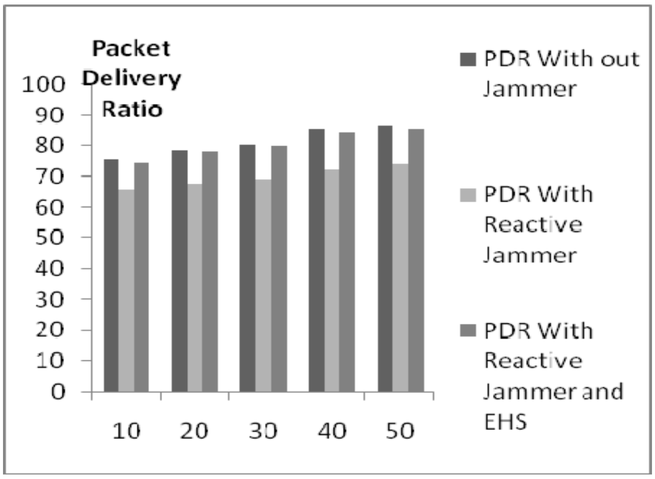

Fig 4a. Performance analysis in terms of PDR

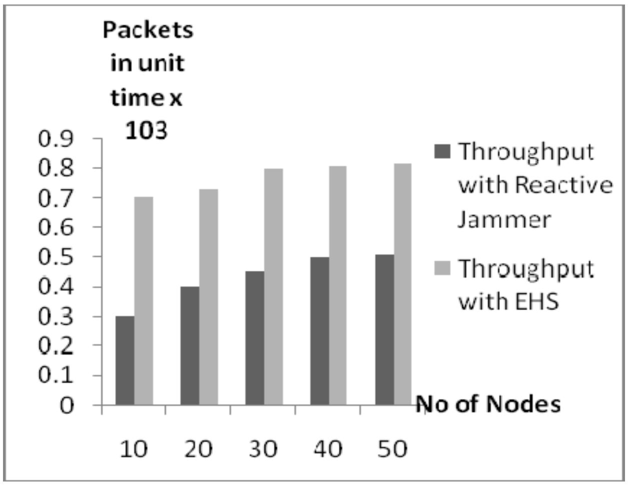

Fig 4b .Performance analysis in terms of throughput

V Conclusion

We addressed the problem encountered by the nodes in Mobile Adhoc Networks because of reactive jammer. We have considered jammer as an internal part of the network thus being aware of all the network secrets. An effective hiding mechanism was proposed to encounter such type of jammer. Our observation show that the jammer can classify transmitted packets in real time with very less effort.

Though the adversary is present within the network, implementing the above proposed methodology we are able to provide an effective hiding mechanism which make the transmission of the packets in the open wireless media so secure. To analyze the security of our schemes metrics for computational cost and communication overhead were considered. The adversary is prevented to access the data with a mechanism which has less computational overhead and communication cost. So with the adopted methodology against reactive jammers the nodes were able to defend their transmission in Manets.

References

[1]. Alejandro Proaño, Loukas Lazos, Packet-Hiding Methods for Preventing Selective Jamming Attacks IEEE Transactions on Dependable and Secure Computing pp. 101-114, 2012.
[2]. Anthony D. Wood and John A. Stankovic (2004), A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks, IEEE.
[3]. O.Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.
[4]. Kanika Grover, Alvin Lim, Qing Yang. Jamming and Anti-Jamming techniques : A Survey International Journal of Adhoc and Ubiquitous computing ,pages 197-215, 2014.
[5]. Gavin Yeun, Mineo Takai, Rajive Bagrodia Alireza Mehrnia, Babak Daneshrad. Detailed OFDM Modeling in Network Simulation of Mobile Ad Hoc Networks, Parallel and distributed simulation, pages 26-34,2004.
[6]. L. Lazos, S.Liu and M.Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169-180 ,2009.
[7]. Krishna Suthar, Prof G J Sahani. Energy Efficient Routing In Mobile Adhoc Networks: A Survey International Journal of Engineering Research &Technology.
[8]. D.Stinson. Cryptography: theory and practice. CRC press, 2006.
[9]. R.Rivest, A.Shamir, and D.Wagner. Time-lock puzzles and timed-release crypto. Massachusetts Institute of Technology, 1996.
[10]. 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.