Method for preventing Selective Jamming Attacks

Umesh Kumar Awasthi, K. John Singh
School of Information, Technology and Engineering, VIT University, Vellore-632014, TamilNadu, India

Abstract- Wireless medium provides high speed wireless connectivity so, it is more vulnerable to interference attacks, called as jamming attack. This jamming interference in wireless transmissions of data can generate a DoS attacks on wireless networks. With the protocol specification knowledge and network secrets knowledge, one can reduce the efforts of jamming, so that jamming is difficult to detect and counter. Here, the addressed problem is jamming of signals in wireless transmission. Advantages of selective jamming can result in the performance degradation of system and adversary. These results are depicted by two case studies; the foremost is selective attack on routing followed by TCP attack. Security of these methods and computational overhead are also examined.

Keywords- Jamming; Routing attack; TCP attack; Adversary; DoS attack

I. Introduction

In these days wireless network is increasingly becoming more easy to afford, and accordingly are being spread in many modalities, laying out from wireless LAN to sensors and mesh networks. These types of networks are becoming popular, because these networks are providing better security and trustiness. Security and trust are critical and important issue during the transmission. In the wireless data transmission it is easy to generate security threat with the help of proper network security designed architecture. For this there is need of making some necessary changes in the security services, which can be confidentiality of data, authentication of users and integrity of wireless environment. Wireless networks has threat of less security because wireless medium can't be enough covered by using cryptographic rues. Radio interference is the most dangerous form of wireless data transmission threat. As we all know that wireless medium has its open nature, so it can be mixed with the wireless data transmission technologies, so that it can allow wireless data transmission in a broadcast and well monitored way. Antagonists can detect the wireless communication and by putting some unwanted messages or signals they can launch DoS attack. Still, there are more chances to establish to DoS attacks, so that wireless devices are empowered to stop communication.

In the wireless medium data transmission is under threat because it has its open nature. Anyone can detect the ongoing messages with the help of receiver and can put unwanted messages, which can generate problems in data transmission. An important way to degrade the performance of the network is jamming attack. Open medium, which is wireless medium, jamming is a vast problem for data transmission in wireless medium. Jamming is the main factor that can exploit the use of the wireless medium. Jamming produces the denial of service by jamming the particular route which is used for data transmission.

In jamming, the jammer captures transmitted message and send these false message to receiver. Most simple way for jamming is that jammer detects the ongoing messages and he can make some unwanted changes in the operational frequencies of network. Now receiver is unreliable for receiving the messages or it will get false messages.

In most of the wireless medium control data is used for transmitting high protocol data. It works as platform which provides service to user. If control data is not used during the transmission then user can't connect with each other. Therefore control channels are only point which can generate failure of transmission. So, attackers attacks only on control channels and jam them, which produces the DoS attacks.

There are distinctive jamming strategies for jamming the data transmission. In One from them high power interference signals are generated which are in immediate wave manners. Here we can also use FM modulated noise. However, there are many jamming strategy which are known, from them one is "always-on". Following an "always-on" strategy for jamming has many drawbacks. One is that, to jam all the frequency jammer has to use more energy. Second, there can be the continuous presence of high interference levels to detect "always-on". Another one is that these types of attacks are very easy to extenuate by spatial retreats, SS communications, or removal of the jamming nodes and localization.

In jamming, it has one feature that is sensing. In that, there is need of feature of discovering and detection of network, which is transmitting data. Sensors are present in every physical layer, which are used to know the presence of data packets. If there is any encrypted data or network, then only start time of data transmission and packet's size can be measured. Sensor is used for classifying the packets at the upper layers of network. For example, node in 802.11 is used to check that transmitted packet is jammed or not.

If there is a vast network, then attacker can jam the particular part of the network. For getting more gain attacker can attack on these particular part. There is less chance to detect the jammer so, attacked network is not aware for jamming measurement. If jammer is targeting only on some particular TCP data packets, then there can be contradiction between TCP window and less stability of connection so that there can be weak wireless connection or over-crowing of data. Now, attacked users can get the conflicting view of network if, ICMP packets are not blocked.

For launching jamming attacks, here we generate the real time classification of packets in a feasible manner. To generate the maximum effect of attack we choose a attacker which have the knowledge of networks protocols and secrets of nodes. We studied the effect of selective jamming attack on performance of network on TCP protocol.

Here we consider an adversary, which have full knowledge of the networks protocols with their implementation. With this protocol knowledge, the adversary can attack on particular packets which have their higher importance. Example selective jamming attack is TCP acknowledgments jamming which can decrease the speed of data transmission of TCP connection because of congestion control mechanism. Selective jamming is active only for short time of duration so, in this less memory is needed. Main important task for launching selective jamming attack is that adversary which we are choosing should be capable to classifying the packets at the real time and from these packets detect important data. To perform selective jamming, the adversary must be capable to classify transmitted packets in real time and find out important messages and corrupting them. Classification of packets can be done by encoding few bits of packets. Example –Frame of MAC layer with control fields.

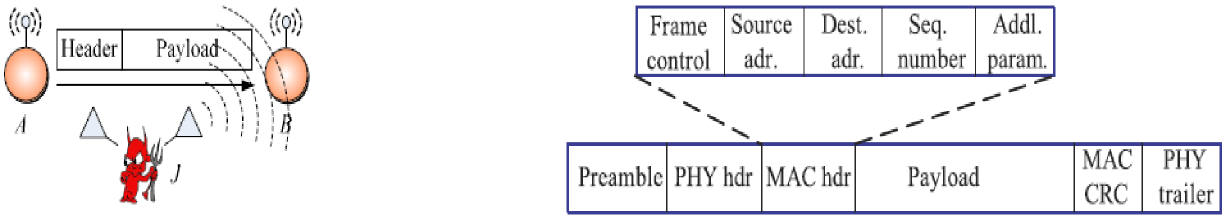

Fig. 1 Recognition of a selective jamming attack and a general frame format in a wireless network

Radio interference attack can't be launched by formal security mechanisms. An antagonist can ignore the protocol of medium access and transmit the packets in a continuous way. By this way, he can prevent the user to begin working with Mac operations. He can also generate collision of packets that can generate repletion of packets. Such types of threats in the MAC-layer and PHY-layer can be known for particular time.

There are many issues that related to weaknesses of MAC-layer in 802.11. These issues are again included by Australian CERT in their current announcement.

To assure the proper transmission of the packets in the wireless medium there should be some mechanisms, which provides the way to deal with all types of threats. First stage to prevent the medium form attacks is that, we have to find out the way, in that particular attack is feasible. After that we have to find out the way to remove these attacks. Here we examine the selective jamming attacks and how they are effecting the wireless transmission of data. An adversary selects the region, which have high importance and then jam the particular route.

II. LITERATURE SURVEY

In [1] Cagalj et al showed that wormholes are considered as a threat but these can be use as a defensive process. For solution of this, they applied channel diversity. In that, if there is jamming attack on the nodes, in this condition these nodes can work for communication route and can avoid the jamming of signals. In the jamming, information flow is uninterrupted. If acknowledgement is not received by the sender after sending the packets more than one times triggers the wormhole creation.

Based on this principle, they explained probabilistic wormholes principle with examining three approaches. Firstly, they explained that, if a network grows with regular wireless sensor nodes with a particular number of sensors nodes pairs then this network will form a hybrid sensor network. In the second part of paper they explained that, nodes which are in distributed form, can arrange themselves same as pairs of frequency hopping. In these two approaches, they assumed that there is minimum one wormhole. They proposed a novel anti-jamming technique.

They considered that wireless sensors network can discover an event. First of all wireless sensors detects the jamming and then it provide this information to network operator. Now network operator will take action according to jamming. If network sensor fails to detect the event then it will not forward this information to the operator. So, this event can make the system unreliable or interrupted.

In [6] Hoesel et al developed a method for jamming attacks in that they use only packets which were in encrypted form. Work only on encrypted packets. These packets are very effective for reactive jamming. These packets use less energy than reactive or random jamming. They use these jamming attacks for showing the properties of data link layer. They showed the result in valued form. These implemented attacks are applicable only for only three particular MAC protocols, but these can be used for other protocols which belong to same category. Proper analysis or study of these attacks provide security from attacks and help in protection from attacks, when there is no efficient countermeasure.

They discussed and showed attack algorithms. They provided the methods for simulation of protocol. Afterwards they showed the methods for evaluating the results of these algorithms. Then they discussed the ways to explores potential countermeasures. In their work, they focused only on LMAC protocol. For this protocol they showed efficient jammer implementation and efficiency of LMAC counter-measure.

In [4] M. Strasser et al discussed about the circular dependency. They divided it into two parts. First one is communication in anti jamming spread-spectrum and another is key establishment when medium is jammed. They proposed a new method “Uncoordinated Frequency Hopping” for the solution of circular dependency. This method provides a jamming-free communication. Further they discussed about the method to apply this scheme in a protocol, which is used for key establishment. This entire process is done, when the jammer is present. This makes nodes to agree on using shared secret key. It enables the nodes to agree on using a shared secret key. This key can be used for “secret frequency hopping” and for communication using “coordinated frequency hopping”.

They described and addressed the anti-jamming technique for circular dependency which was based on shared key distribution. This key is distributed in a jamming free medium. Here one question arises that jammer is present in the medium already, then how is it possible to get a shared key? For giving the answer of this question they give one scheme called as “UTF”. This UTF scheme can distributed the key in the presence of jammer by key establish protocol. Further this key supports in communication.

They launched a model of denial of service attacker. This model detects the jammed signals. It also protects from modification of transmitted data and insertion of unwanted data. This technique provides slower data communication but it gives higher space for storage with higher cost of processing.

In [3] Popper et al concentrated on the anomaly of broadcast communication. They demonstrated a way of broadcast using anti-jamming; with the usage of secret keys that can be shared. This method being employed was quite robust. When there are more numbers of receivers, broadcast transmission is needed. In this case number of un-trusted users can be in any number. In such settings, a sender can communicate with both set of receivers: to un-trusted receivers or to a dynamic set of trusted receivers. In both cases, employing of pre-shared keys to convey the information is an inappropriate alternative. This method helps to re-coordinate the setting by making the nodes to associate with it; hence is clearly based on anti-jamming

They depicted the issue of anti-jamming as a pertinent problem which can be established using shared keys and can be dealt using spread-spectrum techniques in an uncoordinated manner. They aimed at a strategy known as Uncoordinated DSSS. In this scheme, anti-jamming communication is performed without using shared keys and also, communication can take place in settings where DSSS is impossible to be used.

They inspected the execution of UDSSS. They depicted that UDSSS can perform as good as DSSS; but only when jamming is not present and the transmission of messages to ten receivers takes much less time for systems in high jamming areas.

In [5] Tague et al discovered that a jammer with the cognition of the fundamental channel access protocol is able to generate a DoS attack. This attack works by performing jamming operations in all the communicating channels used by individual users or neighborhoods of mobile networks. Furthermore, if the adversary is permitted to distinguish between data and control message channels by access protocol, then the energy required to jam the channels of communication is much less than the optimal energy needed by an attack centering only on control.

They also formulated an agreement between the troubles in wireless networks of establishing keys and accessing of control channels and built up a model for strategies of control channel access furnishing accessibility of control messages assigning the keys randomly. They proposed certain parameters to measure the service accessibility and service quality in the scenarios of jamming of control channels. They accessed these parameters by broadening the existing results and their extension to capturing of nodes in wireless networks. They also proposed certain methods to identify and annul endangered users.

In [2] Tague et al discovered that to jam the control channels, only the cognition of frequency and interval of time is needed. Hence, control channels need to be hidden in frequency bands or time interval with the use of cryptographic primitives. The position of control channel was thus found using hash functions that are keyed.

In such concerned area, they proposed methods to control jamming using distribution of keys randomly. They also evaluated and categorized the performance based on the number of endangered users.

In [7] Noubir et al depicted the multi-hop adhoc network scenario in which the dispersal of small number of smart jammers took place in a geographical area and they could survive with limited energy for a longer period of time. These jammers require short jamming periods; therefore can be used to jam various other channels with the remaining energy and time.

They can also be used to launch an attack focusing on the internodes traffic.

The proposed technique in this paper is fully focused on the perfect assembly of error correction codes and cryptographically strong inter-leavers. The fundamental presumption in this research is that a fixed cost is employed to jam a single bit. They found out the effects of these costs in the destruction of an entire packet. To increase and for enhanced resiliency, spread spectrum techniques along with other existing methods can be assembled in a coordinated manner.

III. PROPOSED METHOD

In this work, jamming attacks is shown using two forms of attacks. In wireless medium, attacks take place when data is sent in the form of packets. The first case is route jamming and another one is TCP jamming. In the route jamming, if there is more traffic in a particular route or the attacker has jammed that route, then the source needs to find another route based on Random Walk Gossip protocol. By this protocol, we can find another most suitable route from sender to destination. There can be many routes from a particular sender to destination. From these routes, there will be an alternative route between the same sender and receiver based on priority. Now packets can travel by this high priority alternate route without jamming.

Another form is TCP attack explained as follows. In this type of jamming, if a packet is transmitted from one node to another, the receiver node needs to send acknowledgement after receiving the packets. If the sender is not receiving the acknowledgement within a particular time then, sender will assume it as attack. So now, sender will not send another packet to that node. For transmitting packets, now sender will send these packets to cluster node and this cluster node will forward these packets to destination. So, in this scenario cluster node will work as mediator. Now, packets will be forwarded with the help of cluster node.

When any data is transmitted from sender to destination, then data is fragmented in to packets and RSA algorithm is used for encrypting the data. This encryption technique provides security from other attacks.

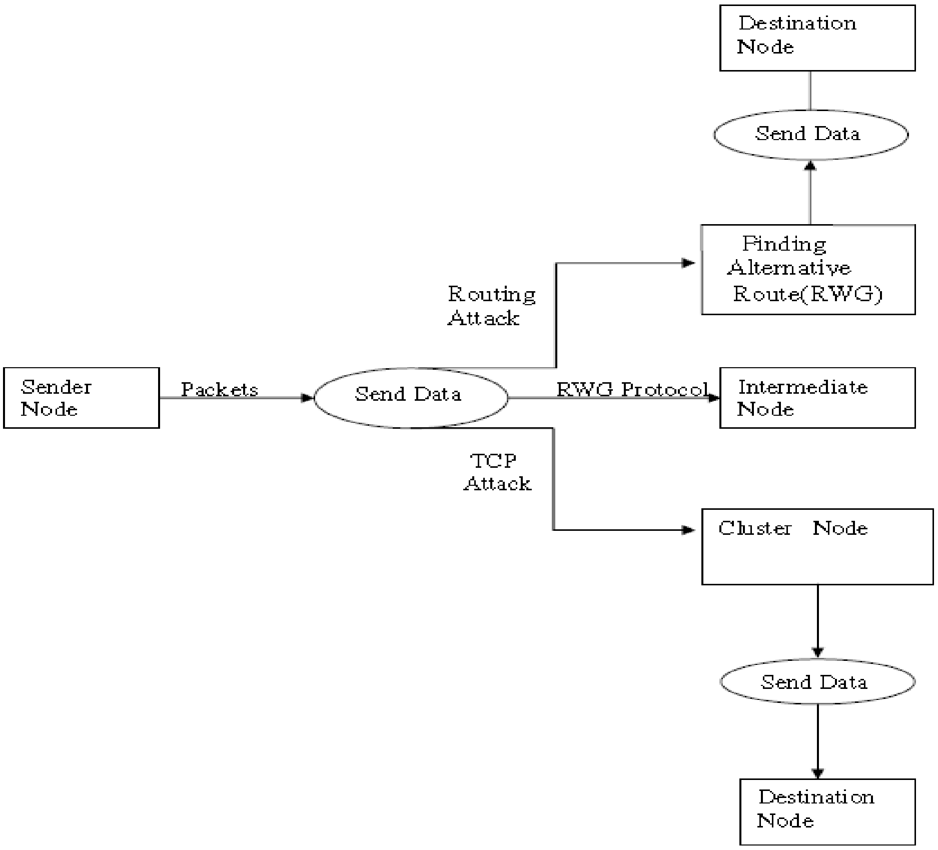

Fig. 2 Architecture diagram of proposed system

IV. CONCLUSION

Here, the anomaly of selective jamming attacks in the scenario of wireless networks is being addressed. An internal adversary model is emphasized in which the jammer forms the part of the network which is under attack. The affect of such jamming attacks is assessed on network protocols like TCP and routing. The observations depict that the performance can be affected by a selective jammer with a considerable amount of effort.

The transmission from the jammed route is prevented with the help of algorithm and TCP attack with the help of cluster node.

REFERENCES

[1] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. MobileComputing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[2] Tague, M. Li, and R. Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," Proc. IEEE Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC), 2007.

[3] C. Popper, M. Strasser, and S. Capkun, "Jamming-Resistant Broadcast Communication without Shared Keys," Proc. USENIX Security Symp., 2009.

[4] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-Resistant Key Establishment Using Uncoordinated Frequency Hopping," Proc. IEEE Symp. Security and Privacy, 2008.

[5] P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009.

[6] Y.W. Law, M. Palaniswami, L.V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-Efficient Link-Layer Jamming Attacks against WSN MAC Protocols," ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38, 2009.

[7] G. Noubir and G. Lin, "Low-Power DoS Attacks in Data Wireless Lans and Countermeasures," Mobile Computing and Comm. Rev., vol. 7, no. 3, pp. 29-30, 2003.