Volume 2, Issue 11, November 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Analysis on Denial of Service attacks and Packets Defending Methodologies in Wireless Sensor Networks

K.Manojkumar
Dept of Computer Science and Engg
K.S.R.College of Engineering,
Tiruchengode, India

M.Vinoth kumar
Assistant Professor,
K.S.R.College of Engineering,
Tiruchengode, India

Dr.G.Tholkappia Arasu
Principal
A.V.S Engineering College
Salem, India

Abstract - Security measures have been proposed to identify, isolate, mitigate and prevent the Denial of Service attacks in Wireless Sensor Networks. The wireless networks are preferred over the traditional approaches for its faster accessibility, connectivity, and compatibility among the extended variant set of users.Yet the need of authenticating the frames in wireless networks has been ignored for better transfer rate. This shortens the limitations of the existing wired networks and global applicability promoted the implementation. Wireless Sensor Networks are subjected to various attacks from jammers of all nature. The detection strategies sometimes fail to analyze and report the presence of a jammer in a network. Detection of the jammers is quite easy in case of external locality since they possess a significant pattern of attack and route to attack the victim. On the other hand, being unconscious of the detection mechanisms, the external jammers always provide a trace to be detected. Being an internal attacker, the node would have adequate understanding over the present defensive mechanism and additional tools to masquerade their identity. In view of protecting the packets against the jamming attacks, various methodologies are implemented for disguising and secrete the message packets from the jammers. Concealing the packets enables a safe transmission between intended nodes even in the existence of an active jammer.

Index terms: Defending mechanisms, Network Security, Jamming, secrete packets, DoS attacks, internal jammers.

I. INTRODUCTION

Wireless Sensor Networks succeeded much theoretical impossibility and simplified the architecture of the networks implementation. The networks established using traditional approaches has significant conditions on extension of the nodes or sensors and connecting the nodes via physical cables. The expenditure and constraints were too difficult to be obeyed in the traditional approaches of implementing a network. On the other hand, the wired networks were too stringent over the attackers too. The entry procedure of any user is clearly monitored which restricted many imperfect attackers. Speaking of the attackers in the wireless networks in internet services specifically, there has been no limit to be defined. High accessibility and usability made the wireless networks a bit insecure to that of wired networks. Limited access with physical links is thus a secure method to protect the resources of a network from external users. But in a view of a large organization, there is a serious necessity of providing access to multiple users with easier protocols [3].

Internet has been proven to be a good solution for every doubt of any user. The boundless internet services provide accessibility to every user who possesses connectivity. Designed for simplicity and accessibility, the immense structure of internet is far easier to obtain services from. Similar to that a private network can establish its framework for multiple users through wireless medium. Wireless communication between the nodes and server needs a transceiver of prescribed frequency [13] and appropriate authentication. This permits the attackers to easily enter and block the services of the original users. The open structure of the wireless networks facilitates the attackers to enter and exit with less effort. Compromising the nodes and acting as the legitimate user is also possible with enough details on the authentication codes. Disclosures of the secret codes even in the presence of highly secure algorithms would invite the attackers. Independent nodes in the networks are taken over by the knowledge on the internal activities.

Attacks in the wireless networks may be of any kind to disturb the normal functioning of the network. Attacks may block or jam the communication channel [7], corrupt the packets, inject wrong messages, flood the medium with false messages or simply eavesdrop the activities of the networks. Any of these attacks would greatly influence the control and efficiency of the wireless networks. Measures have to be taken immediately to identify, isolate and mitigate the attacks and attacker.

This paper contemplates on the internal attacks, which are considerably more harmful to the network. External attacks are easier to be determined and mitigated since they have a specific outlineof attacks. Their packets can be monitored based on the flow, length and the path selected for transmission. The packets would be intended for either flooding the network and jam the medium to prevent it from being allocated for the right users. These attacks originate from the attackers called

Jammers, who keeps monitoring the network and forward the attack packets into the medium at the right time. The detection strategies would be activated after a stated time of the attacks. The remedial measures are initiated after the effects are severe. Hacking of email accounts would be irrecoverable by the original users. The next section discusses about the attackers who act within the network and the areas of attacks.

II. EXTERNAL VS. INTERNAL ATTACKERS

The attackers are differentiated by their motive. Most recent attacks are classified under jamming, which prevent the normal flow of data and control packets [5]. The attackers may be originated from either a remote location or a within a network based on the type of messages they attack [15] and their type of attacks.

External attackers are adversaries from any location beyond the network. They continuously monitor the network on the packets transferred, the communicating nodes and other mechanisms. The external attackers gain enough knowledge on the activities of the network before striking. They are also concerned about hiding from the detection mechanisms to maintain their attacks. Inadequate knowledge about the network would soon reveal them and mitigate them. Recent attacks conclude that a high power transmitter is enough for exhausting the communication bandwidth assigned for the network communication. The powerful signal from external attackers is enough to produce a Denial of Service (DoS)attack. Similarly instead of a high power radio signal, it could be bulk amount of pointless message packets. A number of false requests to the server can move it to a state in which it completely becomes unstable and would not respond to any of the requests. The intended client is also made to wait to get the response for its request. The ultimate aim of an attacker is to block the services available to the original user.

The mentioned attacks are forwarded from the unrelated attackers of the networks. This paper describes an even more dangerous attack, from the very own member of the network. Internal attackers are compromised nodes or the members of the network itself. The compromised nodes are controlled by an external attacker whereas the member may misbehave to jam the services provided to the other members of the same network. The internal attackers have a strong reason to be superior to the external attackers since they acquire the required knowledge much easier than the former. They would attack the network services just for fun in most cases or to take revenge upon the top level management. An internal attacker would know when and where to attack and thus perfectly plans his activities. This type of attackers on delivering his attack packets into the network would easily protect his identity from the detection mechanisms.

The attackers of the internal kind are active only for a short period of time and thus cannot be monitored for the defined time to identify an attack. Hence it becomes more difficult to determine whether it is an attack or mere loss of packets due to congestion. The internal attacker need not jam the entire bandwidth or flood in the bandwidth as the former attacker, but may target on the messages of high importance such as connection establishment messages, request and response pairs etc. This type of attack is called as selective jamming attacks.

III. DENIAL OF SERVICE (DOS) ATTACKS OF AN INTERNAL JAMMER

Jamming is achieved by flooding the bandwidth [14] or exhausting a network with numerous requests such that it loses concentration on the priority and the order of execution. The service provider will get confused on which to respond first or gets crashed in most cases. Requests of different varieties would not provide a chance for the network to react and thus crashes the whole system.

One has to clearly understand the difference between the congestion in a network and Denial of Service (DoS) attacks. Legitimate requests from multiple users cause congestion. Congestion can be removed by making the requests wait till the state changes. If the intention of the requests sent to the server is defined for making them wait indefinitely, then it is called as the DoS attack. The requests remain unanswered till the congested state is removed, yet the jammer would continuously jam the network by sending in false requests.

The internal jammer or attacker is capable of observing the activities at every moment and act accordingly. They need not be active for a long time to attack. Aware of the detection and prevention strategies, the attacker will stay low till the network functions are degraded. The internal attacker would pose a threat in any of the following means.

Sybil attacks are used to gain the control of the networks by compromising a number of nodes with multiple identities. The internal attacker avails the information of the entities and their session details. All the users are supposed to maintain a pattern of usage of the services in a network. The time a person logins and the type of services he uses is recorded in the space of a network monitor. An internal jammer may know the details on its colleagues or friends or may be capable of hacking the network monitor and recover the recorded information. With the information on the login ids and password the same internal attacker may act as multiple entities and possess as many sessions as possible. Finally the attacker would be able to misuse the resources of the network. The network monitor would validate on the identities of those multiple nodes but not doubt their source. Resulting in a blockage of services to the original users who would be rejected to login and obtain their service.

The next type of attack is the node replication attack by an internal jammer, in which the nodes are created repeatedly with the intention to disturb the original routes in the network. In case of a large organization, the number of nodes is high to obtain services from the server node. The source and the destination nodes cannot communicate directly as they are near at most instances. If the requesting node is at a far end of the boundary, a number of intermediate nodes would be involved in the communication process. The transfer of packets crosses many hops till it reaches the destination node. The nodes are replicated with the same identity such that there are numerous nodes with one identity. When the route is established, there is no surety that the original node will be assigned. The replicated nodes would lead to a false destination thus jamming the original route. This attack is severe if the messages to be communicated are of high importance. The internal jammer would be aware of all the identities of every node on the network.

Wormhole attacks are the next kind of attacks of an internal jammer. The packets transmitted at the source node are recorded by the attacker. The jammer would then create a dedicated pathway for the copy of the packets to an attacker's destination node. This method would disturb the confidentiality of the message packets. The worm holes can be also created in between the original source and a duplicate destination by assuring it as a true destination node. In the presence of a wormhole, the source would not be aware of the destination nodes. The jammers are careful enough to hide themselves and be active to become a serious attack. Jammer need not know the keys [1] for breaking the encrypted message for posing a threat since the packets are jammed from reaching the destination which is already an attack. Being an internal attacker the keys [2] used for encryption and decryption would be open to all members of the network. The route request and response messages are the primary concerns of the attacker. Without a secure channel for communication the messages [6] cannot be ensured with confidentiality. Immediate analysis and detection of these wormholes is absolutely necessary to prevent huge data loss.

These fore mentioned attacks concentrate on compromising the nodes and their activities. The next type of attack greatly concentrates on the messages of high importance. A Selective jamming attack wait for the transmission of high significance messages and then block them from reaching the destined nodes. Blockage of these messages requires much less effort than the former type of internal attacks. The internal jammer is well informed about the time and types of the important messages unlike the external attackers.

IV. PREVENTION STRATEGIES FOR INTERNAL JAMMERS

The messages have to be kept secret in order prevent them from being attacked. Determination on the type of message packets makes it simpler for the attacker to categorize and forward their attack packets. They are prone to easier retrieval if their contents are visible. Hence to conceal the packets from being revealed many Cryptographic methods have been proposed for encryption and decryption of the message packets with secret keys. Encryption is a method of transforming the message into some other representations with a key. After the transformation of the message, the original form is hidden from the attackers. Decryption of the message is the reverse process of encryption. With the same key, encrypted message can be retrieved to its original form. There are notable cryptographic methods to transform a message into a secret form. The keys are generated by the source and later disclosed to the destination of the same. Sometimes the keys are private if the messages are highly confidential. The public keys are maintained by all the members of the network [4]. Members of the network are involved in a communication process by the transmission of a message packet and its associated keys used for decryption.

In case of internal attacks, to prevent the disclosure of the keys to the jammer inside, random key generation was proposed to overcome the drawback. Nodes participating in the data transfer alone share the keys for the encryption and decryption of the messages. Random key generation [10] was subjected to the source and destination nodes to protect the keys and thus the message. On-time generation of the keys defines a safe way to transmit the packet even in the presence of an internal jammer. Without the on-time generated keys the internal attacker would not be able to crack the encrypted message between a defined source and destination nodes. There may be multiple hops in between but there is no possibility of possessing the particular key of the encrypted message.Only the node possessing the right key can decrypt the message.

Another method proposed that there is no need for sharing the keys between the nodes. The messages are sent to the destination node after breaking into a number of smaller packets. Each packet is marked with an identity such that only a reassembly of all the packets into a complete message can decrypt the message. The attacker cannot introduce the attack packets as the attacker is unaware of the identity mark defined by the source node [11]. All the attack packets without the identity marks would be considered as the attack packets and can be discarded without any hesitation. The identification of attack packets is easier as the attack packets have typical and different mode of representation. Original packets possess a defined representation known only to the source and destination nodes.

There has been a method to allocate a frequency for transmission of the packets. Frequency hopping methodologies [9] separates a particular frequency hopping for a unit of time and jumps to a next frequency after some time. An attacker cannot predict the right frequency used for transmission between the source and destination node. Since the hopping is not prescribed to predefined values or any order, the allocation is completely random. This makes the attacker to detect the channel and obtain the packets with additional efforts even if he is a part of the network.But this method wastes the total frequency allocated as the whole band is allocated whether used or not. An important question is that can it be dedicated at times of congestion [12]. No is the answer. During congestion the bandwidth is exhausted and the random allocation of bands is not possible. The next interesting method of securing the message packets from the attackers is to hide the entire message in a game or a cryptographic puzzle [4][8]. A game would completely distract the attacker from the attacking mechanisms. Designing and implementing a game requires greater efforts and space over the resources. Another drawback of imposing a gaming technique is, when distributed jammers introduce the attack packets, gaming methods are not efficient to prevent them. A commitment algorithm was proposed to encrypt a message packet with the *Commit* function and a key. This strategy is similar to that of sharing a private key to only the source and destination nodes discussed in previous methodologies. A cryptographic puzzle would encourage the jammer to be indulged in performing the solving activities rather than modes to attack the nodes. The internal attacker would start concentrating on how to solve the puzzles. A reasonable time is necessary for the jammer to concentrate and crack the messages. This time is computed to be equivalent for the message to be delivered to the right node. If the packet is blocked, retransmission strategies would be initiated. Meanwhile the message would reach the destination safely. This process would considerably involve huge computations for hiding the packets onto a puzzle or on a commitment.

V. CONCLUSION

This paper discussed about the different Denial of Service (DoS) attacks and the origin of the attacks. Analyzing the source of the attacks should be accurate and quick enough for determining the location of the attackers and mitigating them. The defending strategies proposed are in need of certain alterations to protect and conserve the confidentiality of the message packets. Every method proposed in a conserving ideology rises another new type of attack. Denial of Service attacks raised from the jammers greatly affects the performance of the networks.The attacks are generated to override the present detection and prevention strategies.

REFERENCES

[1] Y. Desmedt, “Broadcast Anti-JammingSystems,” Computer Networks, vol. 35,nos. 2/3, pp. 223-236, Feb. 2001.

[2] O. Goldreich, “Foundations of Cryptography: Basic Applications”. Cambridge. Univ. Press, 2004.

[3] B. Greenstein, D. Mccoy, J. Pang, T.Ko-hno, S. Seshan, and D.Wetherall, “Improving Wireless Privacy with an Identiftifier-Free Link Layer Protocol,” Proc.Int’l Conf. Mobile Systems,Applications,and Services (MobiSys), 2008.

[4] A. Juels and J. Brainard, “Client Puzzles:A Cryptographic Countermeasureagainst Connection Depletion Attacks,”Proc. Network and Distributed SystemSecurity Symp. (NDSS), pp. 151-165,1999.

[5] L. Lazos, S. Liu, and M. Krunz,“MitigatingControl-Channel JammingAttacks in Multi-Channel Ad HocNetworks,” Proc. Second ACM Conf.Wireless Network Security, pp. 169-180,2009.

[6] R.C. Merkle, “Secure Communicationsover Insecure Channels,” Comm. ACM,vol. 21, no. 4, pp. 294-299, 1978.

[7] C. Popper, M. Strasser, and S. _Capkun“Jamming-Resistant BroadcastCommunication without Shared Keys,”Proc. USENIX Security Symp., 2009.

[8] R. Rivest, “All-or-Nothing Encryptionand the Package Transform,”Proc. Int’lWorkshop Fast Software Encryption, pp.210-218, 1997.

[9] M. Strasser, C. Popper, and S. _Capkun, “Efficient Uncoordinated fhssAnti-Jamming Communication,” Proc. ACMInt’l Symp.MobileAd Hoc Networking and Computing(MobiHoc), pp. 207-218, 2009.

[10] P. Tague, M. Li, and R. Poovendran,“Probabilistic Mitigation of Control
Channel Jamming via Random KeyDistribution,” Proc. IEEE Int’l Symp.Personal, Indoor and Mobile RadioComm. (PIMRC), 2007.

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

[12] W. Xu, W. Trappe, and Y. Zhang,“Anti-Jamming Timing Channels forWireless Networks,” Proc. ACM Conf.WirelessNetwork Security (WiSec),pp.203-213, 2008.

[13] M. Strasser, C. Po¨pper, S. _Capkun,and M. Cagalj, “Jamming-ResistantKey Establishment UsingUncoordinated Frequency Hopping,”Proc. IEEE Symp. Security andPrivacy, 2008.

[14] T.X. Brown, J.E. James, and A. Sethi,“Jamming and Sensing of EncryptedWireless Ad Hoc Networks,” Proc.ACM Int’l Symp.Mobile Ad HocNetworking and Computing(MobiHoc), pp. 120-130,2006.

[15] Alejandro Proano and Loukas Lazos.“Packet-Hiding Methods for Preventing Selective Jamming Attacks”.IEEE Transactions on dependable and secure computing, Vol. 9, No. 1, January/February 2012.