IJCTA, 9(36), 2016, pp. 221-227
© International Science Press

An Efficient Jammer Revocation on OLSR Network

S. Britto Raj* and V. Khanna**

Abstract : The wireless medium is very open to transfer information and this openness leads attackers to create jamming. This process is known as an external threat model. The current schemes encompass cryptographic primitives such as commitment scheme, cryptographic puzzles and allor- nothing transformation with physical-layer attributes. Though it is secured, it has some loopholes to attack the packets. To avoid these attacks,we propose a new system which addresses these selective jamming attacks under internal threat.To restrict this internal threat, the proposed system uses a blowfish algorithm which efficiently hides the packets and its classification from the adversaries. Here we used the distance based process and it is for the non centralized process. So here the route discovery process is somewhat difficult under the malicious attacks.OLSR is link stability based routing protocol for supporting Mobile Ad hoc Network. It chooses the next hop based on the link stability. So it is more efficient than the AODV for detecting such attacks.

Keywords : Selective jamming, Wireless network, Packet Classification, Link State Routing.

1. INTRODUCTION

Wireless Network depends on continuous connection of interconnecting engaged nodes.The open nature of this medium will lead the adversaries to attack packets which are not hidden. The attackers will make selective jamming on the wireless network. While passing the packets, the attackers will wait on the network for a short period and attack the selective information. Due to this attack, the Denial-of-Service may occur on the network. The attackers will be outside of the network. It is known as an external threat or attack.Though the attackers attack from the outside, without having some internal knowledge, they cannot make this attack.

In order to avoid this situation, the current system creates three schemes. The schemes combine cryptographic primitives such as commitment scheme, cryptographic puzzles and all-or-nothing transformation with physical-layer attributes. This scheme made the transferring of packets in a secured way. But it still has some loopholes to make the attackers to create selective jamming. In this paper, in order to secure the transferring of packets without any attack, the OLSR algorithm is introduced. This algorithm provides high security to the packets transferring.

2. REALATED WORK

2.1. Problem Statement

Consider this problem : Two nodes A and B communicate via a wireless channel. Within the communication distance of both A and B there is a jamming node J. When A carries a packet m to B, node J analyzes m by receiving only the first few bytes of m. J then corrupts m beyond recovery by snooping with its induction at B. We address the problem of averting the jamming node from classifying mean real time, thus reducing

* Dean, Information, Bharath University

the J’s ability to work selective jamming. Our goal is to transform a selective attacker to a random one. Note that in the present work, we are not addressing packet classification methods based on protocol semantics.

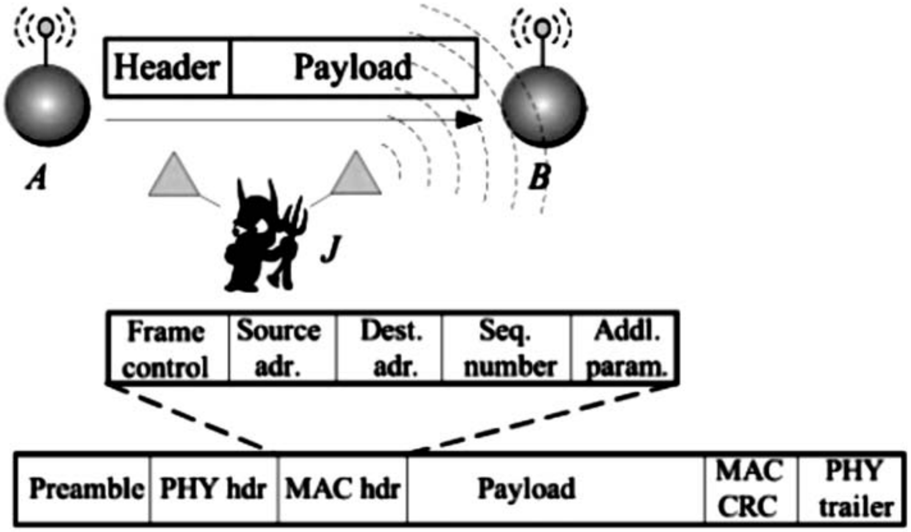

Figure 1: Jamming in network

2.2. System and Adversary Model Network model

The network exits of a collection of nodes associated through wireless channel. Nodes may interact directly if they are within corresponding range, or indirectly via multiple bands. Nodes convey both in unicast mode and broadcast mode. Communications can be either decrypted or encrypted. For collated broadcast communications, balanced keys are shared among all pinned receivers. These keys are embedded using already accumulated pairwise keys or asymmetric cryptography.

2.3. Communication Model

Packets are transmitted at a rate of R bauds. Each PHYSICAL-layer symbol corresponds to *q* bits, where the value of q is defined by the underlying digital modulation scheme. Every symbol carries __ *q* data bits, whereα/β is the rate of the PHYSICAL-layer encoder. Here, the transmission bit rate is equal to QRbps and the information bit rate is __ QRbps. Spread spectrum techniques such as a direct sequence spread spectrum (DSSS) may be used at the PHYSICALlayer to protect wireless transmissions from jamming. SS provides resistance to interference to some extent (typically 20 to 30 dB gain), but a strong jammer is still able to perform of jamming data packets of his choosing. Dispatched packets have the general format. The preamble is used for synchronizing the sampling process at the receiver. The PHYSICAL layer header contains information regarding the length of the frame, and the communication rate. The MAC header impels the MAC protocol version, the source and destination addresses, arrays of numbers plus some extra fields. The MAC header is followed by the framework body that typically encompasses an ARP packet or an IP datagram. Conclusively, the MAC frame is assured by a cyclic redundancy check(CRC) code. At the PHYSICAL layer, a trailer may be affixed for organizing the sender and receiver.

Adversary Model

We hypothesize the antagonist is in control of the connection medium and can jam messages at any part of the network of his choosing. The antagonist can achieve in full-duplex approach, thus being able to accept and carry simultaneously. This can be achieved with the use of multi-radio transceivers. Furthermore, the attacker is qualified with directional aerials that acclaim the acknowledgement of a signal from one node and jamming of the same signal at another.For study purposes, we accept that the attacker can actively jam a number of bits just below the ECC adequacy early in the communication. He can decide to unable to be rectified to corrupt a communicated packet by jamming the last attribute. In reality, it has been determined that fussy jamming can be accomplished with far less resources. A jammer endues with a single half-duplex transceiver is acceptable to classify and jam communicated packets. However,our model catches a more potent attacker that can be emphatic even at high communication speeds.The adversary is estimated to be figuring and storage bounded, although he can be far expert to normal nodes. In particular, he can be armed with special purpose hardwarefor performing crypt evaluation or any other required calculation. Solving a well-known hard cryptographic issue is considered to be time-consuming. With the goal of analysis, given a blank text, the most effective method for deriving the relevant plaintext is considered to be an embracive search of the key space. The utilization details of every layer of the network stack are considered to be public. Furthermore, the attacker is capable of physically negotiating network devices and catching up stored information combining cryptographic keys, PN codes, etc. This internal antagonist model is pragmatic for network builders such as mobile ad-hoc,mesh, subjective radio, and wireless sensor networks, where network devices may operate neglected , thus being persuadable to physical compromise.

3. EXISTING CRYPTOGRAPHIC METHODS

In Existing system, jamming has been addressed under an external threat model in which the jammer is not part of the network. A hacker with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. Under this model, jamming strategies include the continuous transmission of high-power interference signals. The existing system adopts an “always-on” strategy. In the simplest form of jamming, the attcker interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Usually, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Since jamming strategies include the continuous or random transmission of high-power interference signals.

Demerits of the existing system are as follows: The strategy used in the existing system is “always-on” strategy which has several disadvantages.

- First, the hacker has to expend a significant amount of energy to jam frequency bands of interest.
- Second, the continuous presence of unusually high interference level sakes this type of attacks easier to detect.

Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

These cryptographic methods, it encompasses three schemes.Cryptographic schemes combine cryptographic primitives such as commitment designs, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics. We estimated the security of our designs and determined their computational and transmission overhead.

4. PROPOSED HIDING TECHNIQUES

4.1. Process permutation

In Strong Hiding Commitment Scheme, the process permutation has done to avoid real time packet classification. In process permutation, the input process is received from the sender. The input process is a file, which is split into a number of files depends upon the size of the given input process (file). For example, if the input file that is the data to be sent is of size 10 KB, the data will be split into 10 files. These split files are stored in a location temporarily for the encryption process. Then, the split files are encrypted using an encryption key. Here the encryption has done using Blowfish algorithm. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was developed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. The encrypted files are the permuted process.

4.2. Strong hiding

In commitment scheme, to avoid real time packet classification, the permuted process is hidden for process transformation. Here we take the permuted process as input for strong hiding. The encrypted files are located in a folder by creating a new folder dynamically whenever we execute the project. The encrypted files are hidden that is compressed.

The hidden permuted process will be permuted again along with the length of the permuted process and the encryption key. As we use blowfish algorithm, we can use a variety of keys each time for process permutation and process hiding. The encryption key is padded to the permuted process. After padding the key and the length of the process, the permuted process is encrypted again for strong hiding. As we are using blowfish algorithm, we can use different keys every time for process permutation.

The blowfish algorithm has a 64-bit block. The execution time does not exceed though it has 448 bits in length. It provides high security for packet transformation. After the re-encryption, the process is transferred to the receiver.

4.3. Puzzle creation

In Cryptographic Puzzle Hiding Scheme, a puzzle is created to hide the given input process. The main idea behind such puzzles is to force the recipient of a puzzle execute a predefined set of computations before he is able to extract a secret of interest. The time condition for attaining 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 PHYSICAL-layer parameters. However, it has higher computation and communication overheads. A puzzle is created to get the decryption key for process conversion. If the puzzle is solved, the receiver can get the decryption key to get the plain text. The puzzle is created on the estimation of hacker's knowledge to solve the puzzle.

4.4. Process hides

The process to be transferred is given by the sender. The input process is split into a number of files and encrypted for transformation. The input process is a file, which is split into a number of files depends upon the size of the given input process (file). For example, if the input file that is the data to be sent is of size 20 kb, the data will be split into 20 files. These split files are stored in a location temporarily for the encryption process. The split files are encrypted using an encryption key. Here the encryption has done using Blowfish algorithm. The encrypted split files are zipped to send to the receiver. During file transfer, the puzzle and the zipped file are sent to the receiver. Hence, the process is hidden in the puzzle to avoid real time classification.

4.5. Aon transformation

In All-Or-Nothing transformation scheme, the receiver can get the plaintext if and only if all the split files received. In AON transformation, the input process to be sent is given by the sender for transformation. The given process is divided into blocks of files and its length is padded to it. 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. 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 in the size of the secret key. Pseudo messages are created for the blocks of files and sent to the receiver. The receiver can get the plain text only if he gets all pseudo messages. He can't get plain text, even a single block out of 10 blocks.

5. OLSR TECHNIQUE

Optimized Link StateRouting Protocol is an efficient routing protocol that follows the novel fisheye routing mechanism. It is a proactive protocol that adopts table driven routing methodology. In OLSR, routing generates appropriate routing decisions by taking the eminence of the global network information. Specifically, information exchange is made often between the closer nodes than the farther nodes. Hence, each node acquires accurate information about neighbors and accuracy of information decreases as the distance from the node increases. Figure 4 reveals the fisheye routing in which the central node gets all information about its immediate neighbors; it will be decreased in progressive nodes.

5.1. OLSR Description

Initially, each node starts with an empty neighbor list and an empty topology table. After initializing local variables, each node in the network invokes the neighbor discovery mechanism to obtain the neighbor details and maintain current neighbor relationships. Following that, the link state packets are distributed using information dissemination mechanism in the network. Each node maintains a database consisting LSP. With that information, the node uses the route computation mechanism to acquire the routing table for the protocol which is updated periodically

5.2. OLSR Function

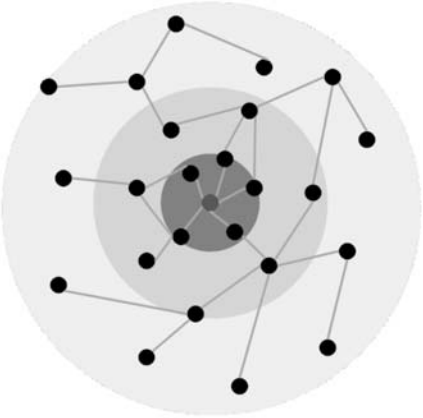

Figure 2

5.3. Routing of OLSR

Generally, the performance of proactive and reactive routing protocols varies with network characteristics and one protocol may outperform the other in different network condition. Further, the optimal routing strategy depends on the underlying network topology, rate of change and traffic pattern. Here, the MRP, which automatically finds the balance point between proactive and reactive routing by adjusting the degree to which route information is propagated proactively versus the degree to which it needs to be discovered reactively. MRP enables each node to use a different application-specific performance metric to control the adaptation of the routing layer. It can also be stated that the application-specific protocols built on top of MRP for minimizing packet overhead, bounding loss rate, and controlling jitter.

5.4. Multi Point Relay (MRP)

In Ad-hoc routing protocols, there is a fundamental trade-off between proactive dissemination and reactive discovery of routing information. While proactive protocols can provide good reliability and low latency through frequent dissemination of routing information, they entail high overhead and scale poorly with increasing numbers of participating nodes. In contrast, reactive protocols, can achieve low routing overhead, but may suffer from increased latency due to on-demand route discovery and route maintenance. Since the characteristics of a practical network vary dynamically with time, choosing an appropriate routing protocol is an important design and implementation decision. A protocol suited for a given network size, density, and mobility may behave inefficiently as the network characteristics and application behavior change. theMutli Point Relay(MRP), which utilizes this fundamental tradeoff between proactive versus reactive routing to find a good balance between route information propagated proactively and route information that is left up to on demand discovery. MRP utilizes both a proactive and a reactive protocol to perform routing. Each MRP node determines the net work neighborhood, called proactive zone, in which routing information pertaining to itself is disseminated proactively. MRP relies on a novel proactive routing algorithm that is both efficient and analytically tractable. Requirements for network performance vary among applications. Multimedia applications can tolerate high loss rates, but are sensitive to variations in delay. TCP traffic is sensitive to loss in the network, while devices running on battery power are concerned with the routing overhead. However, applications have no control over the performance of traditional routing protocols. In contrast, MRP enables each application to pursue different quantitative metrics for guiding the inherent trade-off between increased overhead for proactive information dissemination versus reduced latency and loss rate. Each MRP node can separately pursue different application-specific performance guarantees. For instance, one node may direct MRP to adjust its route dissemination to reduce delay jitter, while another node concurrently uses MRP to minimize packet overhead. MRP enables multiple nodes in the network to pursue disparate goals at the routing layer. The MRP has three significant properties.

- **Adaptive :** The protocol should be applicable to a wide range of network characteristics. It should automatically adjust its behavior to achieve target goals in the face of changes in traffic patterns, node mobility and other network characteristics.
- **Flexible :** The protocol should enable applications to optimize for different application-specific metrics at the routing layer. These optimization goals should not be set by the network designer, but be placed under the control of the network participants.
- **Efficient :** The protocol should achieve better performance than pure, non-hybrid, strategies without invoking costly low-level primitives such as those for distributed agreement or reliable broadcast.

The MRP Hybrid Adaptive Routing Protocol adapts efficiently and seamlessly between proactive and reactive routing strategies. This adaptation is driven by the measured characteristics of the network and can be directed to optimize for user-defined performance metrics, such as loss rate, routing overhead, or delay jitter. Moreover,

MRP adapts between reactive and proactive routing by dynamically varying the amount of routing information shared proactively. It does so by defining a proactive zone around some nodes. A node-specific zone radius determines the number of nodes within a given proactive zone. Each node at a distance less than or equal to the zone radius is a member of the proactive zone for that node. All nodes not in the proactive zone of a given destination use reactive routing protocols to establish routes to that node. Node-specific proactive routing is employed within a proactive zone. Nodes within the proactive zone maintain routes proactively only to the central node.

6. CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We advised an internal attacking model in which the hammer is part of the network under internal attack, thus being aware of the protocol specifications and shared network secrets. We showed that the attacker can classify transmitted packets in real time by decoding the first few symbols of an ongoing communication. We checked out the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective adversary can significantly impact performance with very low effort. We developed an approach to split up the files to transfer the data effectively. The OLSR helps to avoid the attack of packets with the help of producing MPR to retrieve the loss files effectively. This OLSR Algorithm helps in memory utilization and time consuming with the high efficient way comparing with previous techniques. Using the logical ability to solve puzzles by the receiver will help them to retrieve all the files properly. Finally throughput of this OLSR algorithm will help the receiver to receive packets effectively as well as the senders to send their packet with full masking.

7. REFERENCES

1. T.X. Brown, J.E. James, and A. Sethi, “Jamming and Sensing of Encrypted Wireless Ad Hoc Networks,” Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.
2. Y. Desmedt, “Broadcast Anti-Jamming Systems,” Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.
3. G. Lin and G. Noubir, “On Link Layer Denial of Service in Data Wireless LANs,” Wireless Comm. and Mobile Computing, vol. 5, no. 3, pp. 273-284, May 2004.
4. R. Rivest, “All-or-Nothing Encryption and the Package Transform,” Proc. Int’l Workshop Fast Software Encryption, pp. 210-218, 1997.
5. R. Rivest, A. Shamir, and D. Wagner, “Time-Lock Puzzles and Timed-Release Crypto,” technical report, Massachusetts Inst. Of Technology, 1996.
6. M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, “Reactive Jamming in Wireless Networks: How Realistic Is the Threat,” Proc. ACM Conf. Wireless Network Security (WiSec), 2011.
7. M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-Based Anti-Jamming Techniques in Sensor Networks,” IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.
8. B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, “Improving Wireless Privacy with an Identifier-Free Link Layer Protocol,” Proc. Int’l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.
9. L. Lazos, S. Liu, and M. Krunz, “Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad Hoc Networks,” Proc. Second ACM Conf. Wireless Network Security, pp. 169-180, 2009.
10. Challenges and Surveys in Key Management and Authentication Scheme for Wireless Sensor Networks“ in Abstract of Emerging Trends in Scientific Research 2014– 2015. https://ideas.repec.org/s/pkp/abetsr.html
11. R. C. Merkle. Secure communications over insecure channels. Com-munications of the ACM, 21(4):294–299, 1978.
12. M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactivejamming in wireless networks: How realistic is the threat? InProceedings of WiSec, 2011.
13. B. Schneier, Applied Cryptography,John Wiley & Sons, New York, 1994.
14. Security in Wireless Sensor Networks: Key Management Module in EECBKM”Presented in International Conference on World Congress on Computing and Communication Technologies on Feb 27- & 28 and 1st march 2014, on St.Joseph college,TrichyY. Liu, P. Ning, H. Dai, and A. Liu. Randomized differentialDSSS:Jamming-resistant wireless broadcast communication. In Proceedingsof INFOCOM, San Diego, 2010.
15. W. Xu, W. Trappe, Y. Zhang, and T.Wood. The feasibility of launchingand detecting jamming attacks in wireless networks. In Proceedings of MobiHoc, pages 46–57, 2005.