International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 8 Aug. 2015

Implementation of Cryptography based Methods to Prevent Selective Jamming Attacks for True Communication in Wireless Network

Rajesh Kumar Chakrawarti[1], Sonam Choubey[2]
Reader, Computer Science & Engineering, S.V.I.T.S. Indore, M.P. , India[1]
P.G. Scholar, Computer Science & Engineering, S.V.I.T.S. Indore, M.P. , India[2]
rajeshkrchakra@gmail.com[1], sonam297@gmail.com[2]

Abstract: *An absolute solution to selective jamming would be the encryption of transmitted packets with a static key. This is the encryption of packets with packet header. For broadcast communication the static decryption key must be known to all intended receivers. So it is more secure. The open nature of wireless network makes it vulnerable to international interference attacks, commonly referred to as jamming. This jamming with wireless transmission can be used as a launch pad for mounting Denial-of –Service attacks on wireless network. The jamming has been addressed under an external threat model. The adversaries with internal knowledge of protocol specification and network secrets can launch low effort jamming attacks that are difficult to detect and counter.*

Keywords: *Jamming Attack, Denial of Service, Wireless Transmission, Wireless Network Security, External Threat Model.*

1. Introduction

Jamming or dropping attacks have been considered under an external threat model, in which the attacker is not a part of the network. Under this model, jamming methods include the continuous or random transmission of high-power interference signals and attackers can launch low-effort jamming attacks that are difficult to detect and counter. In these attacks, the jammer is active only for a short period of time, selectively aiming messages of high importance. Selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To perform selective jamming, the adversary must be capable of classifying transmitted packets and corrupting them before the end of their transmission. Packet classification is done by receiving just a few bytes of a packet. To launch selective jamming attacks, the jammer must be capable of implementing a classify-then-jam policy before the completion of a wireless transmission. Such method can be actualized by classifying transmitted packets using protocol semantics.

Jamming attacks are much harder to counter and face more security problems. In the simplest form of jamming, the jammer interferes with the reception of messages by transmitting a continuous jamming signal.

2. Existing Approach

In the Existing Method for preventing the selective jamming attacks in wireless Network the packet hiding scheme has been mapped with swarm based protection mechanism (SWPM), which is based on swarm intelligence (SI). In SWPM the transmitter and receiver changes channels in order to stay away from the jammer, this is called Channel Changing Technique. The jammer remains on a single channel changing to disrupt any fragment that may be transmitted in the pulse jamming technique. Using the Swarm based protection technique; the forward agent would be unicast or broadcast at each node depending on the availability of the channel data for end of the channel. If the channel data is available, the agents randomly choose the next hope. As the checked agents reaches the source, the data collected is checked which channel there is prevalence of attacker long time and that are omitted. At the same time the forward agents are sent through other channels which are not detected before for attacks. Using the packet fragmentation the packets are broken into the fragments and transmitted separately on different channels with different SFD. If the fragments are short, the attacker's jamming message doesn't start till transmitter has finished transmitting and hopped to another channel. In future a pre emptive detection policy using honey nodes and a response mechanism based on the existing channel surfing algorithm is used to protect wireless nodes from jammer. Where Honey Nodes create dummy communication at a frequency close to the actual frequency of operation, so that real nodes can jump to another frequency even adversary starts scanning that frequency.

3. Problem Statement

The broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. The wireless medium is open in nature. This makes vulnerable to intentional interference attacks, commonly referred to as jamming attacks. Any person with a transceiver can eavesdrop on wireless transmissions, can inject spurious messages, or can jam legitimate ones. Therefore compromise of a single receiver is sufficient to reveal relevant cryptographic information.

4. Proposed Methodology

An absolute solution to selective jamming would be the encryption of transmitted packets with a static key. For broadcast communications the static decryption key must be known to all intended receivers. So it is more secure. The proposed schemes are as follows:

4.1 Real Time Packet Classification

At the Physical layer, first a packet m is encoded, second interleaved, and then modulated before it is transmitted over the wireless channel. At the receiver end, it is demodulated, de-interleaved and decoded to recover the original packet m. Two nodes A and B communicate via a wireless link. In the communication range of A and B there is a jamming node J.

4.2 A Strong Hiding Commitment Scheme

A strong hiding commitment scheme, it is based on the concept of symmetric cryptography. Let us assume that the sender has a packet for Receiver. First S constructs commit (message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation and k is a randomly selected key of some desired key length s, where the length of k is a security parameter. To recover d any receiver must receive and decode the last symbols of the transmitted packet thus preventing early disclosure of d. When Node A transmits a packet m to Node B, then node J classifies m by receiving only the first few bytes of m. Node J then corrupts m beyond recovery by interfering with its reception at B.

4.3 Cryptographic Puzzle Hiding Scheme

A sender S has a packet m for transmission. The sender selects a key k randomly of a desired length. Then S generates a puzzle (key, time), where function puzzle () denotes the puzzle generator function, and function (t p) denotes the time required for the solution of the puzzle. After generating the puzzle P, the sender broadcasts (C, P). Where C is encrypted message. At the receiver side any receiver R solves the received puzzle to recover key and then computes the decryption to get the m.

4.4 All or Nothing Transformation

A transformation f, which is mapping message m= (m1…..mx) to a sequence of pseudo messages m 1 = (m1 1…..mx 1) is an all or nothing AONT if following properties are satisfied. Where f is a bi-jection (Function).It is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo (Fake) messages is unknown, and f and its inverse are efficiently computable. Packets are preprocessed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo messages corresponding to the original packet have been received and the inverse transformation has been applied.

5. Comparison Parameters

i. Packet Delivery Ratio :
   Packet Delivery Ratio = Total Delivered Packets/ Total Sent Packets
ii. Packet Drop Ratio :
   Packet Drop Ratio = Total Drop Packets/Total Sent Packets
iii. Network Throughput :

N/w Throughput = No. Of Data Packets Received/Time Slot

iv. End To End Delay :
D(end to end) = N[D(trans) + D(prop) + D(proc)]

v. Execution Time : Total Time taken to Execute a Process

vi. Accuracy : Accuracy is Inversely Proportional to the Data Loss

These all six parameters represents to Successful Transmission Ratio, which is directly proportional to successful Prevention Ratio.

6. Comparison Parameters

To insert "Tables" or "Figures", please paste the data as stated below. All tables and figures must be given sequential numbers (1, 2, 3, etc.) and have a caption placed below the figure ("Fig Caption") or above the table("Fig Table") being described, using 8pt font and please make use of the specified style "caption" from the drop-down menu of style categories

Table 1: Comparison Parameter

S No.	***Parameters***	***Proposed Method***	***Existing Method***
1	Packet Delivery Ratio	Greater	Less
2	Packet Drop Ratio	Less	Greater
3	Network Throughput	Greater	Less
4	End To End Delay	Less	Greater
5	Execution Time	90 Sec	120 Sec
6	Accuracy	80%	70%

7. Graphs

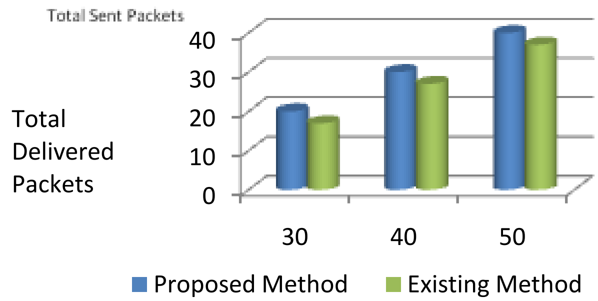

Fig. 1: Packet delivery Ratio

In "*Fig. 1*," Packet Delivery Ratio represents the packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. We have calculated this Ratio here Three Times (30, 40, 50 Packets). Every time the PDR Ratio of Proposed Method is greater than Existing Method

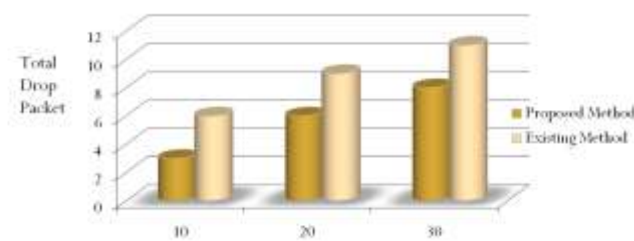

Fig. 2: Packet delivery Ratio

In "*Fig. 2*," Packet Drop Ratio represents the ratio of packets that are not successfully delivered to a destination compared to the number of packets that have been sent out by the sender. We have calculated this Ratio here Three Times (10, 20, 30 Packets). Every time the PDR Ratio of Proposed Method is less than Existing Method.

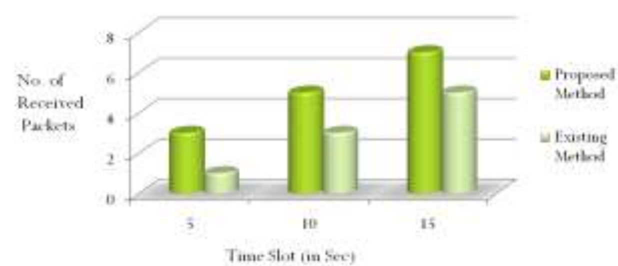

Fig. 3: Network Throughput

In “*Fig. 3*,” Network throughput represents the rate of successful message delivery over a communication channel with respect to Time. We have calculated this Ratio here Three Times (5, 10, 15 Sec). Every time the Network Throughput of Proposed Method is Greater than Existing Method.

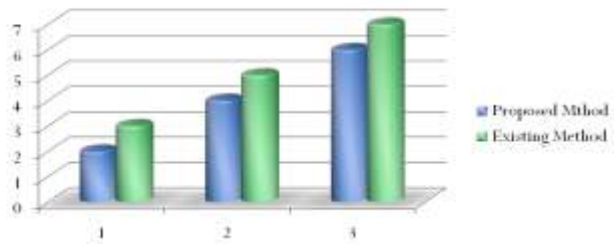

Fig. 4: End To End Delay

In “*Fig. 4*,” End to End Delay represents the average time taken by a data packet to arrive in the destination. We have calculated End to End Delay three times (1, 2, 3 packets). Every time the End to End Delay of Proposed Method is less than Existing Method.

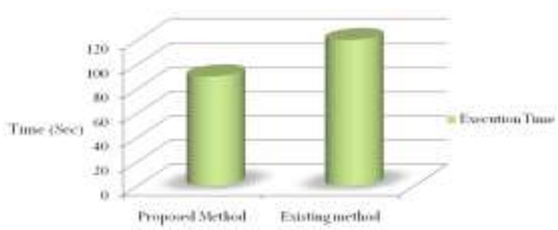

Fig. 5: Execution Time

In “*Fig. 5*,” Execution Time represents here total time (in sec) is taken to execute the particular method. Here Execution Time is 90 Seconds for Proposed Method and 120 Seconds for Existing Method.

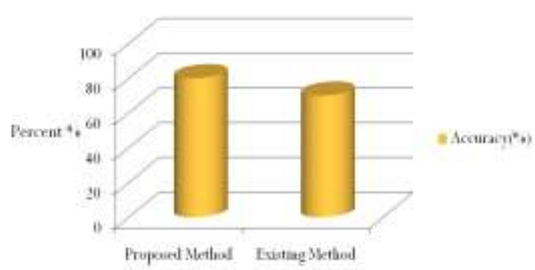

Fig. 6: Accuracy

In “*Fig. 6*,” Accuracy represents here is quality of Method which is based on previous 5 parameters. Here Privacy is 80% for Proposed Method and 70% for Existing Method.

8. Conclusions

In this thesis, we have proposed a cryptography based techniques to prevent the selective jamming Attacks for True Communication in wireless network. It will be more secure because it is based on the concept of static key, which will be used to encrypt the transmitted packets. We showed that the jammer can classify transmitted packets in real time by decoding the first few bits of an ongoing transmission. We evaluated the impact of selective +protocol. Our research shows that selective jammer can significantly impact performance with very low effort. We developed four algorithms that transform a selective jammer to a random one by preventing real time packet classification. Our schemes combine cryptographic primitives such as commitment scheme, cryptographic puzzles and all or nothing transformation with physical layer attributes. We analyzed the security of our four schemes based on six parameters represents Successful Transmission Ratio. We analyzed the overall successful prevention ration which is directly proportional to successful transmission ratio.

9. Future Work

In future proposed method can be improved and implemented on ad hoc Network. Also ‘Elliptic Curve Cryptography’ can be used for more security, That is a approach to approach to public key cryptography, based on algebraic structure of Elliptic Curves over the finite field

Acknowledgments

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings. Especially, please allow me to dedicate my acknowledgment of gratitude toward the following significant advisors and contributors: First and foremost, I would like to thank Prof. Rajesh Kumar Chakrawarti (Department of CSE in SVITS Indore) for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper. Finally, I sincerely thank to my parents, family, and friends, who provide the advice and financial support. The product of this research paper would not be possible without all of them.

References

[1] Alejandro Proano And Loukas Lazos January/February 2012Packet Hiding Methods for Preventing Selective JammingAttacksIEEE TRANSACTIONS ON DEPENDABLE ANDSECURE COMPUTING (vol. 9 no. 1)

[2] Lookas Lazos and Marwan Krunz February 2012 SelectiveJamming/Dropping Insider Attacks in Wireless Mesh NetworksIEEE NETWORK Volume:25 Issue:4 [6] [7]

[3] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang2004Channel Surfing and Spatial Retreats: Defenses againstWireless Denial of Service WiSe '04 Proceedings of the 3rd ACM workshoponWirelesssecurityPages 80-89ACM New York, NY, USA

[4] SudipMisra,Sanjay.K.Dhurander,AvanishRayankulaand DeepanshAgarwal 26-31 Oct. 2008 Using Honeynodes along with ChannelSurfing for Defense against Jamming Attacks in Wireless Networks3rd International Conference on System and Network Communications Page-197-201

[5] Shio Kumar Singh , M P Singh , and D K Singh May to June Issue 2011 A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks International Journal of Computer Trends and Technology Volume 1

[6] T.X. Brown, J.E. James, and A.Sethi, "Jamming and Sensing of Encrypted wireless Ad hoc Networks," Proc. ACM Int'1 Symp. Mobile Ad Hoc Networking and Computing (MobiHoc),pp. 120-130,2006.

[7] M. Cahalj, 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] Y.Desmedt,"Broadcast Anti-Jamming System," Computer Networks, vol. 35,nos. 2/3,pp. 223-226,Feb. 2001.

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

[10] IEEE. IEEE 802.11 standards.ieee.org/getieee802/download/802.11-2007.pdf,2007.

[11] Kwangsung Ju and Kwangsue Chung, Jamming Attack Detection and Rate Adaptation Scheme for IEE 802.11 Multi-hop Tactical Networks, International Journal of Communication Network and Information Security(IJCNIS) vol. 3, No. 2, April,2012.

[12] Mingyan Li, Iordanis Koutsopoulos and Radha Poovendran, Optimal Jamming Attacks and Network Defence Policies in Wireless Sensor Networks, Infocom,2007.

[13] Pusphas Chaturvedi and Kunal Gupta, Detection and Prevention of various types of Jamming Attacks in Wireless Networks,IJCNWC,Vol 3, No 2,May 2013.

[14] G. Sathish Kumar and V. Durgadevi "Providing Network Security by Preventing Selective Jamming Attack" .pp 05-09 in Dec-2012.