ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 9 September 2013 Page No. 2774-2778

Prevention of Selective Jamming Attacks Using Swarm intelligence Packet-Hiding Methods

R.karpagam, P.Archana

Associate professor&Hod, School of Computer science, RVS College of Arts and Science
Coimbatore, Tamil Nadu 641402, India
Karpagam.r@rvsgroup.com

Research Scholar, Department of Computer Science, RVS college of Arts and Science
Coimbatore, Tamil Nadu, India
archusureshp@gmail.com

Abstract
Jamming is one of the most dangerous Pre-arranged disturbance attacks in wireless medium. This attack with wireless transmission is used as a launch pad for rising Denial-of-Service attacks on wireless networks. Usually, electronic jamming has been reportable as AN external threat model. We tend to take into account a sophisticated soul WHO is conscious of network secrets and also the implementation details of network protocols at any layer within the network stack. The soul uses his internal information for launching jam attacks within which specific messages of "high importance" are targeted. To diminish such forms of attacks, we tend to develop 3 schemes that forestall classification of transmitted packets in real time. Our schemes suppose the joint thought of crypto graphical mechanisms with PHY-layer attributes. However during this technique it doesn't prevent the important time packet classification. So, we tend to propose swarm based mostly defense technique for electronic jamming attacks in wireless sensing element networks. Swarm intelligence algorithmic program is capable to regulate amendment in topology and traffic. In channel hoping technique, the transmitter and receiver alter the channels so as to remain far away from the transmitter.

1. INTRODUCTION

Jamming or dropping attacks have been considered under an external threat model [3][7], 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 inactive only for a short period of time, selectively aiming messages of high importance. Selective jamming attacks [1][2][4] 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" [1] 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 continuous jamming signal.

Key Words

Jamming , denial of service ,Swarm intelligence

2. Existing System

The existing system address the of problem jamming under an internal threat model. A sophisticated adversary model in which the adversary is aware of the implementation details of the network protocols. By exploiting this knowledge, the adversary launches selective jamming attacks in which it targets specific packets of "high" importance. selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; The 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 in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet. To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics. Jamming attacks are much harder to counter and more security problems. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by

transmitting a continuous jamming signal, or several short jamming pulses jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high power interference signals.

- The complexity of jamming is the fact that it may not be caused intentionally
- The existing system not prevents the real time packet classification
- The system does not solves the real time classification and not prevent the packet at the time of the attacker
- Jamming can interrupt wireless transmission and occur by mistake in the form of interference, noise or as collision at the receiver or in the circumstance of an attack

3. PROPOSED SYSTEM

The proposed method investigates the impact of selective jamming on critical network functions. Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer. To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. First the problem of real-time packet classification can be mapped to the hiding property of commitment schemes, and propose a packet-hiding scheme based on commitments. Second a packet-hiding scheme based on cryptographic puzzles. 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. Puzzle-based scheme is that its security does not rely on the PHY-layer parameters. It has higher computation and communication overheads. All-or-Nothing Transformations that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivets to slow down brute force attacks against block encryption algorithms .The security of our methods and evaluate their computational and communication overhead. Finally proposed a swarm based defense technique for jamming attacks in wireless sensor networks. Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic.

The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique. The jammers remain on a single channel, hoping to disrupt any fragment that may be transmitted in the pulse jamming technique. Using the swarm intelligence technique, the forward ants either unicast or broadcast at each node depending on the availability of the channel information for end of the channel. If the channel information is available, the ants randomly choose the next hop. As the backward ants reaches the source, the data collected is verified which channel there is prevalence of attacker long time, and those are omitted. Simultaneously the forward ants are sent through other channels which are not detected before for attacks.

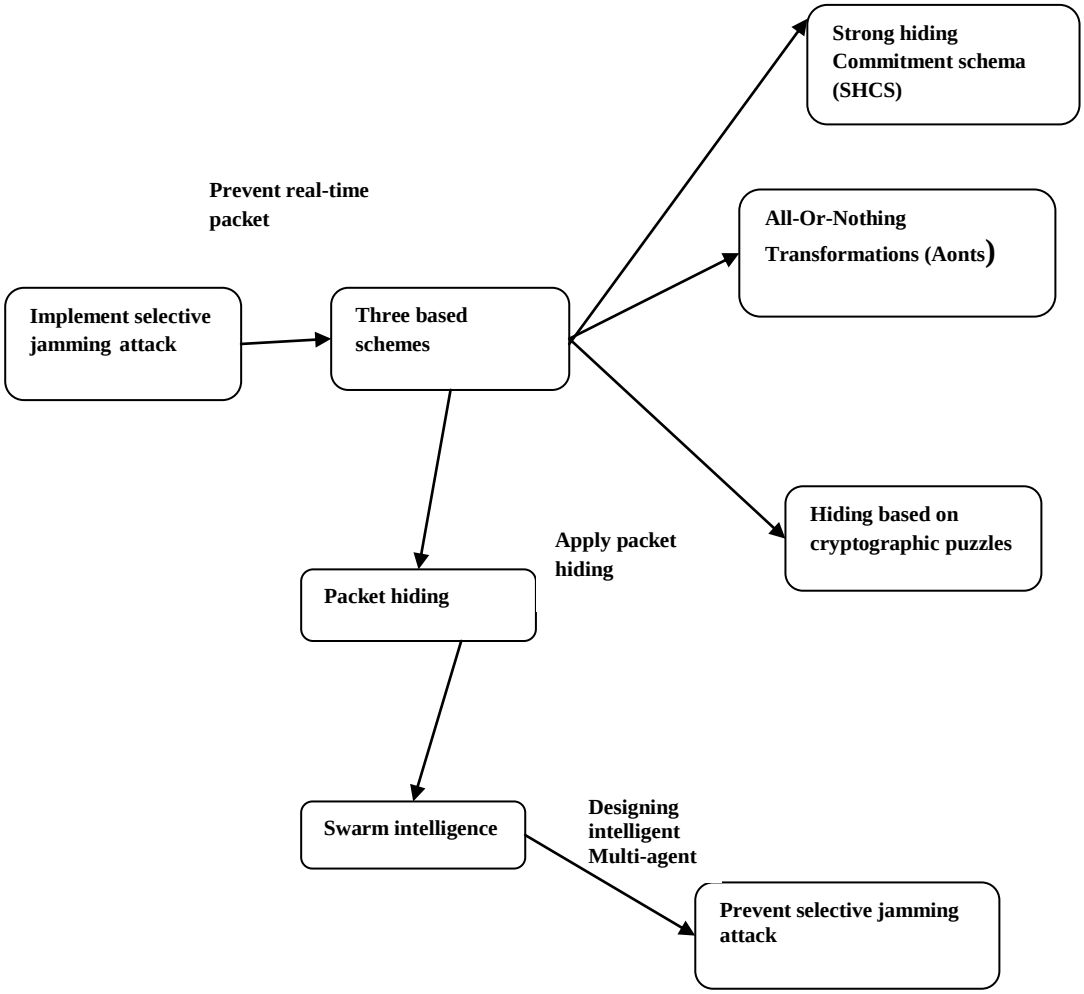
The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique. The pair-wise shared key KS is used for creating a channel key KCh = EKS(1) , which generates a pseudorandom channel sequence. Using packet fragmentation technique, the packets are break into fragments to be transmitted separately on different channels and with different SFD (start of frame delimiter). The last fragment contains a frame check sequence FCS for the entire payload. The time If the fragments are short, the attacker's jamming message does not start till the sender has finished transmitting and hopped to another channel. In the Pulse Jamming attack, the jammer remains on a single channel, hoping to disrupt any fragment that may be transmitted.

- The combination of cryptographic primitives with physical layer attributes for preventing real-time packet classification and neutralizing the inside knowledge of the attacker.
- The proposed system analyzes the security of our methods and evaluate their computational and communication overhead.
- Packet hiding method is used to prevent the selective jamming attack.
- The swarm intelligence technique which updates the sensor details more efficiently and successfully.
- Swarm's forward and backward agents scan through all the channels in a fast way and detect effectively the jamming activity by informing the legitimate node.
- This will improve the detection of a jammer quickly with less complication.
- Swarm Intelligence (SI) is all about designing intelligent multi-agent systems inspired by collective activities of social insects such as ants, bees and wasps

4. Packet HIDING METHODS

Data hiding, this is based on symmetric cryptography. Our main aim is to satisfy the strong hiding characteristics while keeping the computation and communication overhead to a minimum. The proposed SHCS requires the joint consideration of the MAC and PHY layers. To decrease the overhead of SHCS,
the de commitment value d (i.e., the decryption key k) is carried in the same packet as the committed value. This helps to save the extra packet header needed for transmitting individually. To achieve the strong hiding characteristic, a sub layer called the "concealing sub layer" is inserted between the MAC and the
PHY layers. This sub layer is authorized for formatting m before is processed by the PHY layer. A frame m at the MAC layer delivered to the hiding sub layer. Frame m contains a MAC header and a payload, followed by the trailer containing the CRC code. Initially, m is permuted by applying a publicly known permutation _1. The purpose of _1 is to randomize the input to the encryption algorithm and delay the reception of critical packet identifiers such as headers. The computation overhead of SHCS is one symmetric encryption
at the transmitter and one symmetric decryption at the receiver.

4. System architecture



5. Performance evaluations

The existing system addresses the problem of the real time classification. The complexity of jamming is the fact that it may not be caused intentionally. The proposed system analyzes the security of our methods and evaluate their computational and communication overhead. Swarm's forward and backward agents scan through all the channels in a fast way and detect effectively the jamming activity by informing the legitimate node. This will improve the detection of a jammer quickly with less complication. so the propose system improves the performance than the existing system.

a) Route Discovery Time

The average route discovery delay is shown in Fig. 1. This delay is defined as the time difference between the transmission of the first RREQ from a source and the reception of the corresponding RREP from the destination. We observe that the impact of packet hiding on the route discovery delay is minimal compared to the case where no packet hiding is employed.
The following are the graphs of Route Discovery Time that take number of nodes along x-axis and

Route Discovery Time along y-axis. We can infer, as the number of nodes increases, the Route Discovery Time also decreases because there are more route choices for the packet transmission. Among the different response mechanisms are used and we also notice the packets delivery ratio of NH, ME, CS, HP, LT and Swarm intelligence.

Delivery ratio

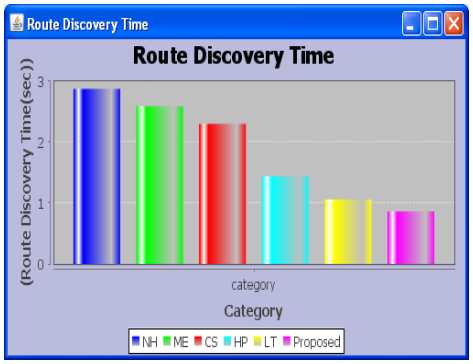


Fig: 1 Route Discovery Time of NH, ME, CS, HP, LT and SWAM

Techniques	NH	ME	CS	HP	LT	SWAM
Delivery ratio	2.8	2.6	2.3	1.5	1.1	0.8

b) Throughput

In Fig. 2, we show the effective throughput. We observe that MAC-layer encryption, SHCS, linear AONT-HS and Swarm intelligence achieve an effective throughput close to the throughput in the absence of packet hiding. This is justified by the relatively small communication overhead of each hiding method and the small queuing delay at intermediate routers due to the absence of any cross traffic. The Swarm intelligence based on the package transform achieved slightly lower throughput, because it occurs a per-packet overhead of 128 bits as opposed to 56 bits. We also observe that hiding techniques based on cryptographic puzzles decrease the effective throughput of the TCP connection to half, compared to the no hiding case. We observe that different algorithm like NH, ME, CS, HP, LT and Swarm intelligence. The proposed system achieves an effective throughput close to the throughput in the absence of packet hiding. The following are the graphs of throughput that take number of nodes along x-axis and delivery ratio along y-axis.

Techniques	NH	ME	CS	HP	LT	SWAM
Throughput	31	33	35	36	38	41

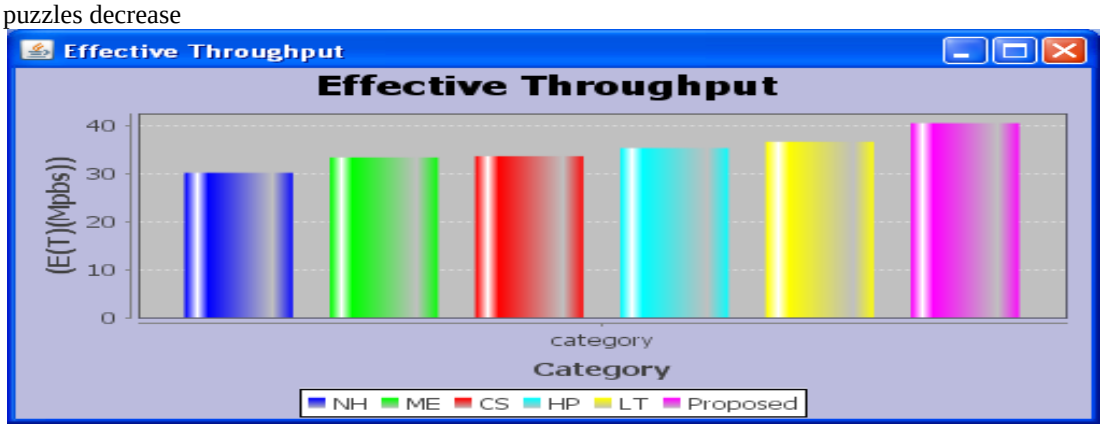


Fig: 8 Throughput of NH, ME, CS, HP, LT and SWAM

6. Conclusion

The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. The proposed method investigates the impact of selective jamming on critical network functions and develops three schemes that prevent classification of transmitted packets in real time. First the problem of real-time packet classification can be mapped to the hiding property of commitment schemes, and propose a packet-hiding scheme based on commitment Second a packet-hiding scheme based on cryptographic puzzles. Finally All -or- Nothing Transformations that introduces a modest communication and computation overhead .A swarm based defense technique for jamming attacks in wireless sensor networks. Finally the swarm intelligence technique which updates the sensor details more efficiently and successfully. This swarm based defense technique for jamming attack is most effective. Using social insect metaphor for solving various problems is the main basisofswarmintelligence

7. Futrure Enhancements

In our enhanced approach, swarm based defense technique for jamming attacks in wireless sensor networks . Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic. The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique. The jammers remain on a single channel, hoping to disrupt any fragment that may be transmitted in the pulse jamming technique. Using the swarm intelligence technique, the forward

Ants either unicast or broadcast at each node depending on the availability of the channel information for end of the channel. If the channel information is available, the ants randomly choose the next hop. As the backward ants reaches the source, the data collected is verified which channel there is prevalence of attacker long time, and those are omitted. Simultaneously the forward ants are sent through other channels which are not detected before for attacks. This scheme helps limit the channel maintenance

8.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) 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.

3) A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

4) T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.

5) Y. Desmedt, "Broadcast Anti-Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.

6) K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009.

7) O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.

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) IEEE, IEEE 802.11 Standard, http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

10) A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999.

11) 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.

12) 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.

13) 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.

14) X. Liu, G. Noubir, and R. Sundaram, "Spread: Foiling Smart Jammers Using Multi-Layer Agility," Proc. IEEE INFOCOM, pp. 2536-2540, 2007.

15) Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication," Proc. IEEE INFOCOM, 2010.