Swarm-based intelligent technique to prevent selective jamming attacks for dynamic topology

S.Surya[1], D.Swathigavaishnave[2], T.Kanimozhi[2]

Assistant Professor, Department of Computer Science and Engineering,

Bannari amman institute of Technology, sathyamangalam, India[1,2,3]

Abstract: Wireless medium is open prone to interference attacks. Jamming is a mode for denial of service attacks on wireless networks. Jamming is an external threat model. Adversaries with internal knowledge of protocol specifications and network secrets initiate low-effort jamming attacks tough to detect and counter. Existing work handle the issue of selective jamming attack in wireless network. Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic. 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. By simulation results, it is clear that this swarm based defense technique for jamming attack is more effective than the existing

Keywords: Jamming attacks, Swarm Based Defense Technique (SBDT), Swarm Intelligence (SI).

I. INTRODUCTION

A. *Wireless Sensor Networks (WSN):*

A wireless sensor network (WSN) constitutes a set of light-weight devices called sensor nodes. It has least energy resources for carrying out the process such as environment sensing, information processing, and communication [1]. A sensor network consists of wireless ad hoc network which means that each sensor supports a multi-hop routing algorithm (quite a few nodes forwards data packets to a base station). Each node in the sensor network is equipped with a radio transceiver or wireless communication device, microcontroller and an energy source (battery) in addition to one or more sensors [2].The wireless sensor network field provides prosperous, multi-disciplinary area of research where a various tools and concepts are engaged for addressing diverse set of application. However, adopting an “al-ways-on” strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect [7]. In this paper, we address the problem of jamming under an internal threat model.The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of “high importance” are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session

B. *Attack:*

WSNs are vulnerable to various forms of intrusions. It needs a solution in distributed and cheap manner in terms of communication, energy and memory requirements. For certain anomalies and applications, typical threats models must be known. The jamming-resistant network could overcome the attack by detecting the jamming, mapping the affected region and routing the jammed area when jamming affects a part of the network [5].

C. *Problem Identification and Solution:*

Among the above discussed different attacks, we consider the jamming attack in this paper and develop a novel detection and defense technique for this attack. 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. Jamming attack is efficient from an attacker's point of view as

An opponent doesn't need special hardware to launch it.
An attack can be implemented by listening to an open medium and distributing in the similar frequency band same as network.
It can lead to significant benefits with small incurred cost for the attacker when launched in a wise manner.
We assume that there are four types of jamming attacks as follows

1) Single-Tone Jammer
2) Multiple-Tone Jammer
3) Pulsed-Noise Jammer
4) ELINT

The network activity becomes poorer as attack can completely remove a coverage area, and in some application network cannot be immediately updated.

.

DEEJAM [8] provides four defensive mechanisms for hiding communication from jammer, evading its search and reducing its impact. But the technique is complex involving complicated calculation and results in more overhead.

Swarm Intelligence (SI) is all about designing intelligent multi-agent systems inspired by collective activities of social insects such as ants, bees and wasps. The agents in the SI system interact directly or indirectly in a distributed troubleshooting way.

Swarm intelligence has the following advantages
- The proximity principle - it carry out simple space and time computation.
- The quality principle - it responds to quality factors.
- The principle of diverse response - it doesn't commit activities along excessively narrow channels
- The principle of stability - does not change its behavior every time as the environment changes.
- The principle of adaptability - it change behavior mote when it is worth the computational price.

II. RELATED WORK

A. Attack Detection Techniques in WSN :

Alegandro praona and loukas [1*]* have proposed cryptography for detecting suspicious transmissions and the consequent identification of malicious nodes and for disseminating this information in the network. They evaluated the detection rate and the efficiency of their solution along a number of parameters. They provided a solution to identify malicious nodes in wireless sensor networks through detection of malicious message transmissions in a network.

B. Real time packet classification:

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J.When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. . This section, describe how the adversary can classify packets in real time, before the packet transmission is completed. Once a packet is classified, the adversary may choose to jam it depending on his strategy

C Strong Commitment Scheme:

Strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. The SHCS requires the joint consideration of the MAC and PHY layers. To reduce the overhead of SHCS, the decommitment value d (i.e., the decryption key k) is carried in the same packet as the committed value C

D . Cryptographic Puzzle Hiding Scheme:

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 required for obtaining 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 PHY-layer parameters. However, it has higher computation and communication overheads. In our context, we use cryptographic puzzles to temporary hide transmitted packets. A packet mis encrypted with a randomly selected symmetric key k of a desirable length s. The key k is blinded using a cryptographic puzzle and sent to the receiver. For a computationally bounded adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming.

III SWARM BASED DEFENCE TECHNIQUE

A.Swarm Intelligence (Si):

Swarm intelligence (SI) is the interaction of simple agents in order to achieve a universal goal. Using social insect metaphor for solving various problems is the main basis of swarm intelligence. Ants, bees, and termites are the insects which live in colonies. Every insect in colony have their own plans. The combination of their activities does not have any supervisor. SI is emerged as combined intelligence of groups of simple agents.
An alternative means of designing intelligent system is offered by SI, so that autonomy, emergence and distributed functioning are replaced control, preprogramming and centralization.
The complex interaction of thousands of autonomous swarm members results in intellectual behavior of SI. The individual ant during food searching process randomly selects the path to proceed. when ants start moving they leave behind a chemical substance called pheromone. Other ants smell and recognize that an ant has visited there before. When the pheromone level is more concentrate, the ant will proceed with that route.

B. General Characteristics of SI:

SI offers characteristics such as adapting network and generating multipath for routing. SI algorithm is proficient enough to adapt change in network topology and traffic and further gives equivalent performance.
It depends on both passive and active information for collective monitoring. They gather non-local information regarding the traits of solution set, like every potential paths.
It utilizes stochastic component like pheromone table for user agents. User agents are autonomous and can interact through stigmergy.
It sets the way in favor of load balancing than pure shortest path. The algorithm also supports multiple paths in order to achieve load balancing.

C. Principle of SI:

There are four principles in swarm intelligent based on which ants will self-organize. They are positive feedback, negative feedback, randomness and multiple interactions.

- Positive feedback- This is helpful in enhancing the good result. The pheromone concentration increases when the ant changes the path from one node to another. This is helpful for other ants to move in this path.

- Negative feedback- This is mainly used to devastate bad results. It is done by decomposing pheromone concentration with respect to time. The rate of decay is trouble specific.
- Randomness - The path selected by ant is in a random manner and thus there is a possibility to generate new results.
- Multiple interactions- By interaction of many agents, the solution is obtained. During food searching process, one ant cannot find the food since pheromone decays. However more ants can find food sooner.

D. Proposed Detection Algorithm:

Step 1
The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique

Step 2
The pair-wise shared key KS is used for creating a channel key KCh = EKS(1) , which generates a pseudorandom channel sequence

$Ch_s = \{E_{KS}$ (i)mod Ch.$\}$, i > 0,

Where, Ch is the number of channels available in the band, message mi is transmitted on channel Chi , (unknown to any but the two parties involved.)

Step 3
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.

Step 4
If the fragments are short, the attacker's jamming message does not start till the sender has finished transmitting and hopped to another channel.

Step 5
In the Pulse Jamming attack, the jammer remains on a single channel, hoping to disrupt any fragment that may be transmitted. As packets cannot be detected quickly enough for selective jamming, the attacker transmits blindly in short pulses.

Step 6
The forward ants (FA) explore the network to collect the jammer's information on each channel. It keeps collecting the attackers' data if any and moves forward though channels. When the FA reaches the end of the channel, it is deallocated and the backward ant (BA) inherits the stack contained in the FA.

Step 7
The BA is sent out on high priority queue. The backward ants retrace the path of the FA utilize
this information to update the data structures periodically.

Step 8
As it 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.

V. CONCLUSION

We proposed swarm based intelligence algorithm for jamming attack .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 help to limit channel maintenance

REFERENCES

[1] Allejandro praona and loukas lazos “Packet hiding methods for preventing selective jamming attack” IEEE transaction vol.9 2012
[2] P. Tague, M. Li and R. Poovendran(2009), ‘Mitigation of Control Channel Jamming under Node Capture Attacks,’IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221-1234.
[3] Strasser M.Popper C.and Capkun, S.(2009), ‘Efficient Uncoordinated fhss Anti-Jamming Communication,’ Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 207-218.
[4] A. Chan, X. Liu, G. Noubir and B. Thapa(2007), ‘Control Channel Jamming : Resilience and Identification of Traitors,’Proc. IEEE Int’l Symp. Information Theory (ISIT).
[5] P. Tague, M. Li and R. Poovendran(2007), ‘Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution,’Proc. IEEE Int’l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC).
[6] M. Cagalj, S. Capkun, and J.-P. Hubaux(2007), ‘Wormhole - Based Anti- Jamming Techniques in Sensor Networks,’IEEE Trans. Mobile Computing, vol. 6, no. 1, pp.100-114..
[7] Thuente D. and Acharya M.(2006), ‘Intelligent Jamming in Wireless Networks with Applications to 802.11 b and Other Networks,’ Proc. IEEE Military Comm. Conf. (MILCOM)
[8] Xu W. Trappe W, Zhang Y.and Wood T.(2005), ‘The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,’Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 46-57.
[9] Xu W. Wood T.Trappe W. and Zhang Y. (2004), ‘Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service,’ Proc. Third ACM Workshop Wireless Security, pp. 80-89.