Selfish Jammer Detection in Multiple P2P Communication Networks

J.Thanushya[1] Prof. E. Evelyn Tabitha[2] S. Abdul Khather[3]
[1]PG Scholar [2,3]Assistant Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]PET Engineering College, India

Abstract— Cooperating jamming is an opportunistic communication technology designed to help the source node send the data simultaneously to cooperative node can selfish jammer node detected in multiple p2p communication networks. Selfish cooperative nodes are a serious security problem because they significantly degrade the performance of a P2P communication networks. The proposed work provides selfish cooperative jammer detection technique, called COOPON, which will detect the attacks of selfish cooperative nodes by the cooperation of other legitimate neighboring nodes. The COOPON algorithm make use of the autonomous decision capability of an ad-hoc communication network based on exchanged information among neighboring nodes.Our proposed COOPON selfish jammer node detection method is very reliable since it is based on deterministic information. We focus on selfish jammer node of neighboring nodes toward multiple p2p communication networks.

Key words: Jammer, Security, Jamming Detection and Packet Drop, Wireless Sensor, Network, Eavesdropper

I. Introduction

The fundamental characteristic of wireless networks that renders them vulnerable to attacks is the broadcast nature of their medium. This exposes them to passive and active attacks, which are different in their nature and objectives [1]. In the former ones, the malicious entity does not take any action apart from passively observing the ongoing communication that is, eavesdropping with the intention to intervene with the privacy of network entities involved in the transaction. On the other hand, in active attacks the attacker is involved in transmission as well. Depending on attacker objectives, different terminology is used. If the attacker abuses a protocol with the primary goal to obtain performance benefits itself, the attack is referred to as misbehavior. If the attacker does not directly manipulate protocol parameters but exploits protocol semantics and aims at indirect benefits by unconditionally disrupting network operation, the attack is termed jamming or Denial-of-Service (DoS), depending on whether one looks at the cause or the consequences of it. Misbehavior in wireless networks stems from the selfish inclination of wireless network entities to improve their own derived utility at the expense of other nodes' performance deterioration, by deviating from legitimate protocol operation at various layers. The utility is expressed in terms of consumed energy or achievable throughput on a per link or end-to-end basis.

Eavesdropping is a well-known security risk for wireless P2P communications, including device-to-device (D2D) link or sideline in cellular networks. Physical layer security against eavesdropping, as described by Wyner in his seminal work, has recently regained substantial research attention. More detailed discussions on recent advances in “physical layer security” can be found in a variety of references. Following a similar physical layer security approach, friendly neighbor nodes can be recruited to serve as cooperative relays or jammers to protect the peer-to-peer signaling link and overcome security vulnerabilities. Traditionally, security enhancement is considered by assuming static transmission links between the source and destination nodes. However, this assumption is not always practical. For example, the selected source node must have the desired data of the destination node.

Wireless Sensor Networks (WSN) receives increasing attention due to their wide application in military as well as in living life [2]. The most essential applications are monitor systems, such as military monitor system or security service system. These applications can allow some normal messages lost in a short period. It cannot tolerate the lost of numerous packets or critical event messages. The attacker deploys the jammers randomly to jam the area. The jammers can disturb the communication between sensor nodes or launch the radios frequency to interfere open wireless environment. Although the jammers are randomly deployed, the damage on the monitor systems is still markedly. The lost of some crucial messages may destroy the entire system.

II. Proposed System

The previous detection method was heuristic simulated annealing algorithm. A simulated annealing (SA) approach is presented to approximately optimize the performance bounds, a one-dimensional search for joint power optimization is further given to further reduce complexity without noticeable performance loss. The content helpers and content requester may form P2P links to share content files for offloading cellular traffic. Traditional scenarios assume static transmission links between the source and destination node. The proposed work provides selfish cooperative jammer detection technique, called COOPON, which will detect the attacks of selfish cooperative nodes by the cooperation of other legitimate neighboring nodes. The COOPON algorithm make use of the autonomous decision capability of an ad-hoc communication network based on exchanged information among neighboring nodes. OLSR Protocol is an optimization of a pure link state protocol for mobile ad-hoc networks. Which we call as Optimized Link State Routing (OLSR).It reduces the size of control packets and minimizes the flooding of this control traffic by using only the selected nodes. This protocol is particularly suitable for large and dense networks, as an optimization done using the multipoint relays work well in the context. More optimization is achieved as compared to the normal link state algorithm. The protocol does not require a reliable transmission for its control messages: each node send its control messages periodically, and can sustain a loss of some packets from time to time.

A. Dijkstra's algorithm

One algorithm for finding the shortest path from a starting node to a target node in a weighted graph is Dijkstra's algorithm. The algorithm creates a tree of shortest paths from the starting vertex, the source, to all other points in the graph. The graph can either be directed or undirected. One stipulation to using the algorithm is that the graph needs to have a nonnegative weight on every edge.

1) Advantage:

- Autonomous and cooperative characteristics for better detection reliabilities.
- Reduce computational complexity of the power optimization.
- Higher Reliability.
- Lower Complexity.

Selfish node detection technique was implemented in NS2 based on COOPON to detect some misbehavioours of the node in the communication links, and also identify the eavesdropper node malicious packet dropping of cooperative legitimate neighbor nodes.

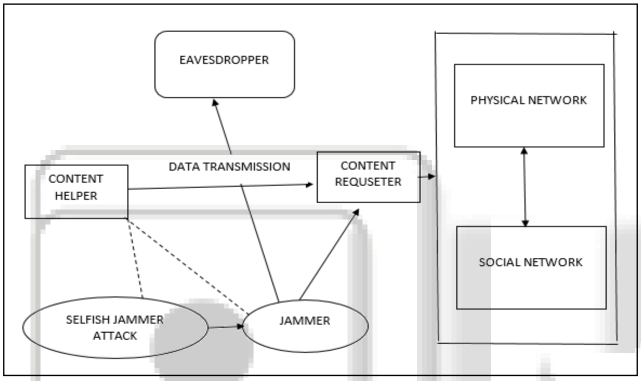


Fig. 2.1: System Architecture

Figure 2.1 describe the architecture of data transmission with the help of jammer and detect the selfish node and the eavesdropper node.

The content helpers are act as source of this transmission to transmit the packets to the content requester. These are done by following steps

- First step is to select the content helper and content requester node in all (1-40) nodes.
- The second step is network formation, here nam files are created and turn on tracing route to generate transport connection between the nodes.
- Third step is route maintenance for topology discovery to finding new path for data transmission previously detect the malicious node in this path then stop message transmit to the source node. This way we drop the malicious node in transmission path.
- Next step is to detect selfish jamming node according to the misbehaviors of the node like as negative role of jammer, this detection done by COOPON Technique to make the use of autonomous decision capability of communication based on exchanged information among neighboring nodes.Misbehaviour changes are calculated based on the packet delivery ratio, throughput and drop.
- Finally eliminate the selfish nodes from the legitimate coordinate neighboring nodes and also dropping eavesdropper node from the decided path or in any node.

The jammer controls the probability of jamming and the transmission range in order to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by the network (namely by a monitoring node), and a notification message is transferred out of the jammed region. Some hosts may misbehave by failing to adhere to the network protocols, with the intent of obtaining an unfair share of the channel. The presence of selfish hosts that deviate from the contention resolution protocol can reduce the throughput share received by well-behaved hosts. The following phases are explain the working of detection techniques using jammer and to preventing the problem.

B. Network Formation

Network Formation using NS2, First Generate nam files and Turn on tracing. After tracing will start then Create network topology to transmit the information in any legitimate path to Create transport connections and finally Generate traffic. Each node must detect all the neighbor nodes with which it has a direct and bi-directional link. The Control Messages (CM) is transmitted in broadcast mode. Each node periodically broadcast its HELLO messages, containing the information about the neighbors and all link status. These are received by all one-hop neighbors, but they are not relayed to further nodes.

C. Route Maintenance

In this module involves finding a new path for the data transmission. Previously detecting the malicious node/nodes on the path, it is informed to the source node. Source node stops sending data packets and checks out its route cache for an alternative path with highest rating value if available. Otherwise, find a new path by initiating route discovery process. In this route discovery process previously detected malicious nodes are avoided so that the new path found will not contain suspected malicious nodes. Dijkstra's algorithm creates a tree of shortest paths from the starting vertex, the source, to all other points in the graph. In Dijkstra's algorithm, this means the edge has a large weight the shortest path tree found by the algorithm will try to avoid edges with larger weights. If the student looks up directions using a map service, it is likely they may use Dijkstra's algorithm, as well as others. Mesh topology is used create a topological representation of network domain during the data transmission.

D. Malicious Packet Dropping

In this module for network optimization MPR (Multi Point Relay) known as set of neighboring nodes are used to spread the link state information. Topology Control messages(TC) are used to broadcast link state periodically. In one hop neighbors each node selects its MPR for minimizing the retransmissions by reaching all its neighbors in two hop. Broadcasting of TC messages lead to the construction of the network with partial topology in which non neighbors are also included in the route. A malicious node causes packet drop in the network by claiming it as the MPR even though it is not. It sends TC messages and leads to packet dropping since routing services are dependent on MPR in OLSR (Optimize Link State Routing) Protocol

E. Preventing Selfish Jamming Attack

Selfish jamming attack is As soon as it receive the packet from neighbor the attacker drop the packet. In some other selfish jamming attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Selfish jamming attack is also termed as node misbehaving attack. Avoidance of selecting suspected nodes as a sole MRP, which is crux of COOPON, mainly prevents the selfish jamming attack. An improvement of COOPON increases the number of received message and minimizes the damage caused by the attack.

F. Attack Detection Model

The network employs a mechanism for monitoring network status and detecting potential malicious activity. The monitoring mechanism consists of: 1) determination of asubset of nodes M that act as monitors, and 2) employment of a detection algorithm at each monitor node. The assignment of the role of monitor to a node is affected by potential existing energy consumption and node computational complexity limitations, and by detection performance specifications.

This paper fixes attention to a specific monitor node and the detection scheme that it employs. First, it need to define the quantity to be observed at each monitor. In this case, the readily available metric is the probability of collision that a monitor node experiences, namely the percentage of packets that are erroneously received. During normal network operation and in the absence of a jammer, it consider a large enough training period in which the monitor node learns the percentage of collisions it experiences as the long-term limit of the ratio of number of slots where there was collision over total number of slots of the training period. A detection algorithm is part of the detection module at a monitor node; it takes as input observation samples obtained by the monitor node (i.e., collision/not collision) and decides whether there is an attack or not.

After each observation at the kth stage, choose between the following options: accept one or the other hypothesis and stop observing, or defer decision for the moment and obtain another observation k + 1. In SPRT, there exist two thresholds a and b that aid the decision. The computed figure of merit at each step is the logarithm of the likelihood ratio of the accumulated sample vector until that step. In this case, the test is between hypotheses H_0 and H_1 that involve Bernoulli with probability mass functions (p.m.fs.) f_0 and f_1 defined by $Pr(c=1) = \theta_i=1 - Pr(C=0)$ where c = 1 denotes the event of collision in a slot. That is, H_0 concerns the hypothesis about absence of jamming with Bernoulli p.m.f. f_0 with parameter θ_0, while H_1 corresponds to the hypothesis of jamming with a Bernoulli p.m.f. f_1 with parameter θ_1. Thus, the logarithm of likelihood ratio at stage k with accumulated samples $x_1,\ldots..,x_k$ is:

$$S_k = \ln \frac{f1(x1,\ldots\ldots xk)}{f2(x2,\ldots\ldots xk)}$$

Where $f_1(x_1,\ldots.x_k)$ is the joint probability mass function of sequence $(x_1,\ldots.x_k)$ based on hypothesis Hi, for I = 0,1. The decision is taken based on the following criteria:

$Sk > a$: accept H_1, $Sk < b$: accept H_0,
$b \leq Sk < a$: take another observation.

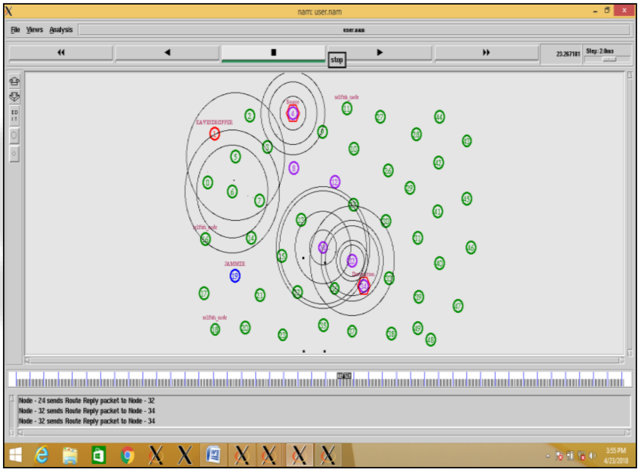
The objective of the detection rule is to minimize

The objective of the detection rule is to minimize the number of required observation samples to derive a decision about existence or not of jamming. The detection performance

III. RESULTS AND DISCUSSION

A. Dropping Eavesdropper and Detecting Selfish nodes

The eavesdropper node will be dropped by the jammer node. To detecting the selfish nodes based on their misbehaviors of the data transmission to send the route reply message between the nodes. Relay messages between nodes, to advertise link state information for their MPR selectors. It can form a route from a given node to any destination in route calculation. The eavesdropper node will be identify by the misbehavior of nodes in the cooperative nodes. If any misbehaviors identified between the selected node then that node will be dropped. Any selfish node detected then the node will be eliminated and perform the secured transmission. Malicious nodes to damaging other nodes by causing network outage. Selfish nodes do not directly intend to damage other nodes, do not cooperate. Relay messages between nodes, to advertise link state information for their MPR selectors. It can form a route from a given node to any destination in route calculation.

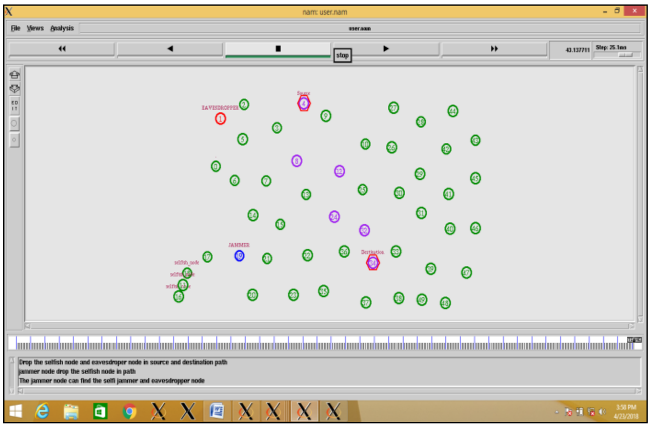


Node - 24 sends Route Reply packet to Node - 32
Node - 32 sends Route Reply packet to Node - 34
Node - 32 sends Route Reply packet to Node - 34

Fig. 3.1: Detecting selfish nodes

B. Eliminating Selfish node to Preventing Selfish Jamming Attack

Selfish node will be removed in the path of data transmission with the help of removing misbehavior nodes of jamming using COOPON technique. Some other selfish jamming attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Selfish jamming attack is also termed as node misbehaving attack. Topology Control messages (TC) are used to broadcast link state periodically. In one hop neighbors each node selects its MPR for minimizing the retransmissions by reaching all its neighbors in two hops. Broadcasting of TC messages lead to the construction of the network with partial topology in which non neighbors are also included in the route. A malicious node causes packet drop in the network by claiming it as the MPR even though it is not. It sends TC messages and leads to packet dropping since routing services are dependent on MPR in OLSR



Drop the selfish node and eavesdroper node in source and destination path
jammer node drop the selfish node in path
The jammer node can find the selfi jammer and eavesdropper node

Fig. 3.2: Eliminating selfish nodes

IV. Conclusion and Future Work

By using the deterministic channel allocation information, COOPON which gives very highly reliable selfish attack detection results by simple computing. The proposed reliable and simple computing technique can be well fitted for practical use in the future. A new approach is designed for cognitive radio ad-hoc networks. This make use of ad-hoc network advantages such as autonomous and cooperative characteristics for better detection reliabilities. For future work cryptographic model and game theory to do theoretical analysis of more than one selfish SU in a neighbor, which gives less detection accuracy.

References

[1] Akyildiz .F, W. Su, Y. Sankara subramaniam, and E. Cayirci, “A survey on sensor Networks”, Communications Magazine IEEE, Vol. 40, issue.8, Aug. 2002, pp. 102–114.

[2] Awerbuch .B, A. Richa, and C. Scheideler, “A Jamming-Resistant MAC Protocol for Single-Hop Wireless Networks,” in Proc. Of Principles of Distributed Computing, 2008.

[3] Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B.Thapa, “On the Performa nce of IEEE 802.11 under Jamming,” in Proc. of IEEE INFOCOM, 2008.

[4] Cagalj .M , S. Capkun, and J.-P. Hubaux, “Wormhole-Based Anti- Jamming Techniques in Sensor Networks,” IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 1-15, Jan. 2007.

[5] Coskun, E. Cayirci, A. Levi, and S. Sancak, “Quarantine Region Scheme to Mitigate Spa m Attacks in Wireless Sensor Networks,” IEEE Trans. Mobile Computing, vol. 5, pp. 1074-1086, Aug 2006.

[6] Dragalin .V.P, AG. Tartakovsky, and V.V. Veeravalli, “Multihypothesis Sequential Probability Ratio TestsPart I: Asymptotic Optimality,” IEEE Trans. Information Theory, vol. 45, no. 7, pp. 2448-2461, Nov. 1999.

[7] Jung, V. Paxson, A.W. Berger, and H. Balakrishnan, “Fast Portscan Detection Using Sequential Hypothesis Testing,” Proc. IEEE Symp Security and Privacy, 2004.

[8] Mallik .R, R. Scholtz, and G. Papavassilopoulos, “Analysi s of an On- Off Ja mming Situation as a Dynamic Game,” IEEE Trans. Comm., vol. 48, no. 8, pp. 1360-1373, Aug. 2000.

[9] McCune .J.M, E. Shi, A. Perrig, and M.K. Reiter, “Detection of Denial-of-Message Attacks on Sensor Network Broadcasts,” Proc. IEEE Symp. Security and Privacy, 2005.

[10] Mingyan Li, Member, IEEE, Iordani s Kout sopoulos, Member, IEEE, and Radha Poovendran, Senior Member, IEEE.. Optimal Jamming Attack Strategies and Net work Defense Policies in Wireless Sensor Networks in IEEE transactions on mobile computing, vol. 9, no. 8, August 2010.

[11] Negi .Rand A. Perrig, “Jamming Analysis of MAC Protocols,”Carnegie Mellon Technical Memo, 2003.

[12] Radosavac .S, I. Kout sopoulos, and J.S. Baras, “A Framework for MAC Protocol Misbehavior Detection in Wireless Networks,” Proc. ACM Workshop Wireless Security (WiSe), 2005.

[13] Wang .L, S. Bashar, Y. Wei, and R. Li, “Secrecy enhancement anal- ysis against unknown eavesdroppering in spatial modulation, ” IEEE Communications Letters, vol. 19, no. 8, pp. 1351-1354, Nov. 2015

[14] Wang .L, H. Wu, and Z. Han, “ Wireless distributed storage in socially enabled d2d communications,” IEEE Access, vol. PP, no. 99, pp. 1-1, 2016.

[15] Wyner .D, “The wire-tap channel,” Bell System Technical Journal,vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[16] Xu .W et al., “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” MobiHoc ’05: Proc. 6th ACM Int’l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46–57.

[17] Xu .W, W. Trappe, and Y. Zhang, “Channel Surfing: Defending Wireless Sensor Networks from Interference,” in Proc. Of Information Processing in Sensor Networks, 2007.

[18] Xu .W, W. Trappe, Y. Zhang, and T. Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” Proc. ACM MobiHoc, 2005.

[19] Xu .W, T. Wood, W. Trappe, and Y. Zhang, “Channel Surfing:Defending Wireless Sensor Networks from Interference,” Proc. IEEE Int’l Conf. Information Processing in Sensor Networks (IPSN),

[20] Yue .J, C. Ma, H. Yu, and W. Zhou, “Secrecy-based access control for device-to-device communication underlaying cellular networks,” IEEE Communications Letters, vol. 17, no. 11, pp. 2068-2071, Nov. 2013.