AN OVERVIEW OF JAMMING TRANSMISSION, DETECTION AND NOTIFICATION USING HEURISTIC ALGORITHM.

Ramalingam Sugumar¹; Tamilenthi.S² and Janet Rajeswari.A.¹

1.Christhuraj College, Trichy, Tamilnadu, India. 
E-mail: rsp_sugu74@yahoo.co.in

Received:16 th,Nov , 2012; Revised: 28 th,Nov,2012; Accepted: 18 th,Jan,2013.

Abstract

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. The jammer is detected by employing an optimal detection test based on the percentage of incurred collisions. On the other hand, the network defends itself by computing the channel access probability to minimize the jamming detection plus notification time. The necessary knowledge of the jammer in order to optimize its benefit consists of knowledge about the network channel access probability and the number of neighbors of the monitor node. Accordingly, the network needs to know the jamming probability of the jammer. Monitoring node gives the message about the jamming region.

Knowledge about the networks and efficient jamming strategy by using heuristic algorithm. A perfect knowledge by both the jammer and the network about the strategy of each other and the case where the jammer and the network lack this knowledge. The latter is captured by formulating and solving optimization problems where the attacker and the network respond optimally to the worst-case or the average-case strategies of the other party. Extending the problem to the case of multiple observers and adaptable jamming transmission range and propose a meaningful heuristic algorithm for an efficient jamming strategy.

Key words: Jamming, Transmission, Detection and Heuristic Algorithm.

INTRODUCTION

We consider one attacker, the jammer, in the sensor network area. The jammer is neither authenticated nor associated with the network. The objective of the jammer is to corrupt legitimate transmissions of sensor nodes by causing intentional packet collisions at receivers. Intentional collision leads to retransmission, which is translated into additional energy consumption for a certain amount of attainable throughput or equivalently reduced throughput for a given amount of consumed energy. In this paper, we do not consider the attacker that is capable of node capture.

We derive the optimal attack and optimal defense strategies as solutions to optimization problems that are faced by the attacker and the network, respectively, by including in the formulation energy limitations. For attack detection, we provide a methodology and an optimal detection test that derives decisions based on the percentage of incurred collisions compared to the nominal one. We include in the formulation the attack detection and the transfer of the attack notification message out of the jammed area. We capture the impact of available knowledge of the attacker and the network about the other’s strategies. For the case of partial knowledge, the attacker and the network optimize with respect to the worst-case or the average-case strategy of the other. We extend the basic model to the case of multiple monitoring nodes and controllable jamming transmission range and suggest a simple efficient jamming strategy.

Analysis Network

We initiate a fixed-length walk from the node. This walk should be long enough to ensure that the visited peers represent a close sample from the underlying stationary distribution. We then retrieve certain information from the visited peers, such as the system details and process details. It acting as source for the network. In sender used to create sends the request and received the response and
destination used to received the request and send the response for the source.

**Routing**

When the packets are sending from the source, they are transferred to the destination through the routers. Routers check for the IP address given by the source with their own IP address for the destination confirmation.

**Multiple Routing**

It is desirable to allow packets with the same source and destination to take more than one possible path. This facility can be used to ease congestion and overcome node failures. To operate such a scheme consistently nodes must maintain routing tables.

Multipath routing allows the establishment of multiple paths between a single source and single destination node. It is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance) or to provide load balancing. Load balancing is of especial importance in MANETs because of the limited bandwidth between the nodes.

**Attacker Model**

This is any entity that is allowed by a data server to provide content services in response to requests by clients. Intermediaries include caching proxies and transforming proxies. They check for the IP address and the packet security by providing content filtering. This module deals with the intruder identification. If an intruder enters the network group, the intruder is identified and the location of the intruder is displayed to the receiver side.

**Optimal Path Selection**

OPSAM (Optimal Path Selection Algorithm for Multicast) for the static multicast routing problem and the newly defined mobile multicast routing problem. The problem is modeled as one of finding the most probable feasible path, where link weights are random variables. A "backward-forward" heuristic is proposed which again uses prelabeling of the graph in the backward direction followed by a forward search that attempts to minimize an objective function. Simulations are conducted to evaluate the performance of the proposed algorithms and to demonstrate the advantages of the probabilistic path selection approach over the classic trigger-based approach.

**Heuristic Algorithm**

The term heuristic is used for algorithms which find solutions among all possible ones. These algorithms, usually find a attackers or jamming, the solution close to the best one and they find it fast and easily. Sometimes these algorithms can be accurate, that is they actually find the best solution, but the algorithm is still called heuristic until this best solution is proven to be the best. The method used from a heuristic algorithm is one of the known methods, such as greediness, but in order to be easy and fast the algorithm ignores or even suppresses some of the problem's demands.

**OVERVIEW OF LITERATURE**

The route discovery is finished once a route from the source node to the packet’s destination is discovered, or all the possible routes to the destination node have been examined. After the route has been found it is kept up-to-date with route maintenance operations until the destination or source node becomes unavailable or the route is no longer desired (Royer, 1999).

Misbehavior can be divided into two categories (Yang, 2006) routing misbehavior (failure to behave in accordance with a routing protocol) and packet forwarding misbehavior (failure to correctly forward data packets in accordance with a data transfer protocol).

There has also been some work that aims to protect data packet forwarding against malicious attacks in order to provide reliable network connectivity. The final part of this section describes some approaches that detect malicious behavior in the data forwarding phase. WATCHERS (Watching for Anomalies in Transit Conservation: a Heuristic for Ensuring Router Security) (Bradley et al., 1998) is a protocol designed to detect disruptive routers in fixed networks through analysis of the number of packets entering and exiting a router. Although WATCHERS is based on the principle of conservation of flow in a network in the same way as our proposed algorithm, its design focuses only on fixed networks and is not applicable to mobile ad hoc networks.

SCAN (self-organized network layer security in mobile ad hoc networks) (Yang et al., 2006) focuses on securing packet delivery. SCAN nodes monitor their neighbors by listening to packets that are forwarded to them. The SCAN node maintains a copy of the neighbor’s routing table and determines the next-hop node to which the neighbor should forward the packet; if the packet is not overheard as being forwarded, it is considered to have been dropped.
In contrast, in our algorithm nodes do not need to overhear transmissions to and from any neighbor in order to detect misbehavior. In SCAN each node must possess a valid token to be able to interact with the network. SCAN develops this idea from (Kong et al., 2001) where tokens are used to give a valid key to a new node entering the network. Similar techniques have also been studied in various papers such as (L. Zhou, and Z. Haas., 1999) where they are used to achieve distribution of trust throughout a network.

Several anomalies can occur in the wireless sensor network that can impair their functionality. The target field that is supposed to be 100% covered by the densely deployed nodes may have coverage holes, areas not covered by any node, due to random aerial deployment creating voids, presence of obstructions, and, more likely, node failures etc. Similarly, nodes may not be able to communicate correctly if routing holes, areas devoid of any nodes, exist in the deployed topology. Thus the network fails to achieve its objectives if some of the nodes cannot sense or report the sensed data. Some of these anomalies may be deliberately created by adversaries that are trying to avoid the sensor network. These malicious nodes can jam the communication to form jamming holes or they can overwhelm regions in the sensor network by denial of service attacks such as sink/black/worm holes (Anthony et al., 2003, Chris Karlof and David Wagner, 2003) to hinder their operation normally based on trust.

**METHODOLOGY**

In existing system, Attacker abuses a protocol with the 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 Misbehavior stems from the selfish inclination of wireless entities to improve their own derived utility to 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 link or end-to-end basis. The first case arises if a node denies to forward messages from other nodes so as to preserve battery for its own transmissions.

**Disadvantages**

- Packets are buffered in the routers present in the network which causes collapse from undelivered packets arises when bandwidth is continuously consumed by packets that are dropped before reaching their ultimate destinations.
- Retransmission of undelivered packets is required to ensure no loss of data.
- Unfair bandwidth allocation arises in the Internet due to the presence of undelivered.

The proposed system has advantage, The jamming attacks that are easy to launch and difficult to detect and confront, since they differ from brute force attacks. The jammer controls probability of jamming and 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 jamming region. The fundamental tradeoff faced by the attacker is the following: a more aggressive attack in terms of higher jamming probability or larger transmission range increases the instantaneously derived payoff but exposes the attacker to the network and facilitates its detection and later on its isolation.

- Buffering of packets in carried out in the edge routers rather than in the core routers.
- The packets are sent into the network based on the capacity of the network and hence there is no possibility of any undelivered packets present in the network.
- Absence of undelivered packets avoids overload due to retransmission.
- Fair allocation of bandwidth is ensured.

**SYSTEM REQUIREMENTS**

**Hardware Requirements**

- **SYSTEM** : Pentium IV 2.4 GHz
- **HARD DISK** : 40 GB
- **FLOPPY DRIVE** : 1.44 MB
- **MONITOR** : 15 VGA colour
- **MOUSE** : Logitech.
- **RAM** : 256 MB
- **KEYBOARD** : 110 keys enhanced.
Software Requirements

- Operating system: Windows XP Professional
- Front End: Microsoft Visual Studio .Net 2005
- Coding Language: C#.Net 2.0
- Database: SQL Server

ANALYSIS

(i) Sensor Network Model

Sensor network \rightarrow \text{Symmetric transmission and reception}

\text{Node transmits at a fixed power level}

\text{Sense activity due to higher signal strength}

\text{Node within transmission range}

\text{Packets can be generated by higher layers of a node}
(ii) Attacker Model

Attacker → Sensor network area → Authenticated nor associated with the network → Intentional packet collisions at receivers → Collision leads to retransmission

Sensing ability in order to sense ongoing activity → Jammed is not needed
(iii) Attack Detection Model

1. Network status and detection
2. Monitoring mechanism
3. Employment of a detection algorithm at each monitor node
4. Determination of a subset of nodes
5. Employment of a detection algorithm at each monitor node
6. Formulate optimization problems for one or several monitor nodes
7. Fix attention to a specific monitor node
8. Define the quantity to be observed at each monitor
9. Node large enough training period in which the monitor
10. Collisions compared to the learned ratio for that specific interval.
(iv) Security

CONCLUSION

The necessary knowledge of the jammer in order to optimize its benefit consists of knowledge about the network channel access probability and the number of neighbors of the monitor node. Accordingly, the network needs to know the jamming probability of the jammer. Monitoring node gives the message about the jamming region. The jammer is detected by optimal detection based on collision.

A perfect knowledge by both the jammer and the network about the strategy of each other and the case where the jammer and the network lack this knowledge. The latter is captured by formulating and solving optimization problems where the attacker and the network respond optimally to the worst-case or the average-case strategies of the other party. Extending the problem to the case of multiple observers and adaptable jamming transmission range and propose a meaningful heuristic algorithm for an efficient jamming strategy.

A first step towards understanding the structure of these problems, identifying tradeoffs and capturing the impact of different parameters on performance. Interesting issues arise in multi-channel networks. More enhanced versions of attacks can be considered, such as the one with dynamic control of jamming probability to extend detection time. Likewise, the network can adapt channel access probability.

Reference
