# OPTIMAL JAMMING ATTACK STRATEGIES AND NETWORK DEFENSE IN WIRELESS SENSOR NETWORKS

G. Sathish Kumar* & K. Ramamoorthy**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

**Abstract:**

*We consider a scenario where a sophisticated jammer jams an area in which a single channel random-access sensor network operates. 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. We study the idealized case of 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. We also take into account potential energy constraints of the jammer and the network. We extend the problem to the case of multiple observers and adaptable jamming transmission range and propose a meaningful heuristic algorithm for an efficient jamming strategy. Our results provide valuable insights about the structure of the jamming problem and associated defense mechanisms and demonstrate the impact of knowledge as well as adoption of sophisticated strategies on achieving desirable performance.*

**Index Terms:** Jammer & Random Access Sensor Network

## 1. 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. In the former, a malicious entity does not take any action except passively observing ongoing communication, e.g. eavesdropping so as to intervene with the privacy of network entities involved in the transaction. On the other hand, an active attacker is involved in transmission as well. Depending on attacker objectives, different terminology is used. If the 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 at its cause or its consequences.

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.

The latter case occurs when a node prevents other nodes from accessing the channel or from routing messages to destinations by selfish manipulation of the access control and routing protocol respectively. The work in focuses on optimal detection in terms of number of required observations to derive a decision for the worst-case access layer misbehavior strategy out of the class of strategies that incur significant performance losses. The framework captured uncertainty of attacks and the case of intelligent attacker that can adapt its policy to delay its detection.

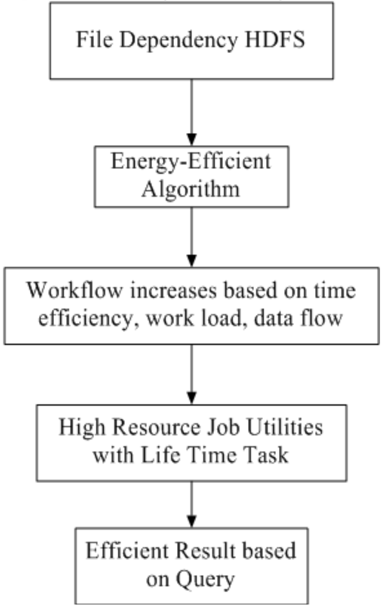

File Dependency HDFS
Energy-Efficient Algorithm
Workflow increases based on time efficiency, work load, data flow
High Resource Job Utilities with Life Time Task
Efficient Result based on Query

Figure 1: Data Flow Diagram

The reminder of this paper is organized as follows. Section II, describes the Related Works. Section III, describes the Proposed Work. Section IV, describes the Experimental Evaluation and Results. Section V summarizes the Conclusion and Future Enhancement.

## 2. Related Works:

Cooperative wireless networking, which is promising in improving the system operation efficiency and reliability by acquiring more accurate and timely information, has attracted considerable attentions to support many services in practice. However, the problem of secure cooperative communication has not been well investigated yet. In this paper, we exploit physical layer security to provide secure cooperative communication for wireless ad hoc networks (WANETs) where involve multiple source-destination pairs and malicious eavesdroppers. By characterizing the security performance of the system by secrecy capacity, we study the secrecy capacity optimization problem in which security enhancement is achieved via cooperative relaying and cooperative jamming. Specifically, we propose a system model where a set of relay nodes can be exploited by multiple source-destination pairs to achieve physical layer security. We theoretically present a corresponding formulation for the relay assignment problem and develop an optimal algorithm to solve it in polynomial time. To further increase the system secrecy capacity, we exploit the cooperative jamming technique and propose a smart jamming algorithm to interfere the eavesdropping channels. Through extensive experiments, we validate that our proposed algorithms significantly increase the system secrecy capacity under various network settings.

## 3. Proposed Work:

One of the most promising ideas is to exploit the wireless channel physical layer characteristics for improving the reliability of wireless transmission against eavesdropping attacks, named as physical layer security. Recently, physical layer security has emerged as a key technique for providing trustworthy and reliable future wireless networks and has witnessed a significant growth. We assume that channels for different pairs of nodes are independent and identically distributed with flat Rayleigh fading, and the noise is the additive white Gaussian noise (AWGN). In the system, a relay node might be compromised to become an eavesdropper, as an inside attacker, which can be detected by its malicious behavior. Some relay nodes will be assigned as jammers to interfere the eavesdropper, while the remaining ones continue relaying information to the destination.

**Advantages:**

- ✓ The secrecy capacity maximization problem in polynomial time.
- ✓ The advantages of cooperative jamming technique are exploited and a smart jamming algorithm is proposed to further increase the system secrecy capacity.

Our proposed algorithms significantly improve the system secrecy capacity under various network settings.

**Modules:**

- ✓ Network initialization for data transmission
- ✓ Data transformation source to destination through nodes
- ✓ Physical layer security to avoid Eaves Dropping
- ✓ Smart jamming algorithm to interfere the eavesdropping channels.

**Network Initialization for Data Transmission:** A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. The network is used for data transfer to the Military Users for Communication to the group of users based on the Coverage range.

**Data Transformation from Source to Destination Through Nodes:** In WANETs network, each source-destination pair can use either direct transmission or cooperative communication with the help of the best relay to achieve full diversity. We define the channel between source and destination and (with or without cooperative relay) as primary channel, and the channel between source and eaves droppers (with or without cooperative relay) as eavesdropping channel. When the direct transmission is applied, the transmission between source and destination can also be overheard by the eavesdroppers. The maximum transmission rate of reliable information secretly sent from the source to the intended destination with the presence of eavesdroppers is termed as secrecy capacity.

**Physical Layer Security to Avoid Eaves Dropping:** Physical layer security for secure cooperative communication, and describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect information from eaves dropping. Physical layer that including new mechanisms that establish cryptographic keys that support communication with assured confidentiality, and that can authenticate transmitters in mobile environments. One can enhance the system security against eavesdroppers by boosting the capacity of the primary channel and simultaneously decreasing the capacity of the eavesdropping one with an efficient relay assignment procedure. Besides, for the relay nodes which are not assigned to help the transmission between sources and destinations.

**Smart Jamming Algorithm to Interfere the Eavesdropping Channels:** Smart jammer is one of the most threat interferences for the GPS receiver. In our model, the jammer is smart and can adjust its transmission power based on the user's transmission power. Based on this fact, we model the power control problem in the presence of a smart jammer as a Stackelberg game, called Power Control with Smart Jammer (PCSJ). In this game, both the user and the jammer are players, of which the user is the leader, and the jammer is the follower. Jammers rely on high transmission power and frequent injection of jamming signals to disrupt communication. Such a strategy is inefficient in terms of jamming power consumption.

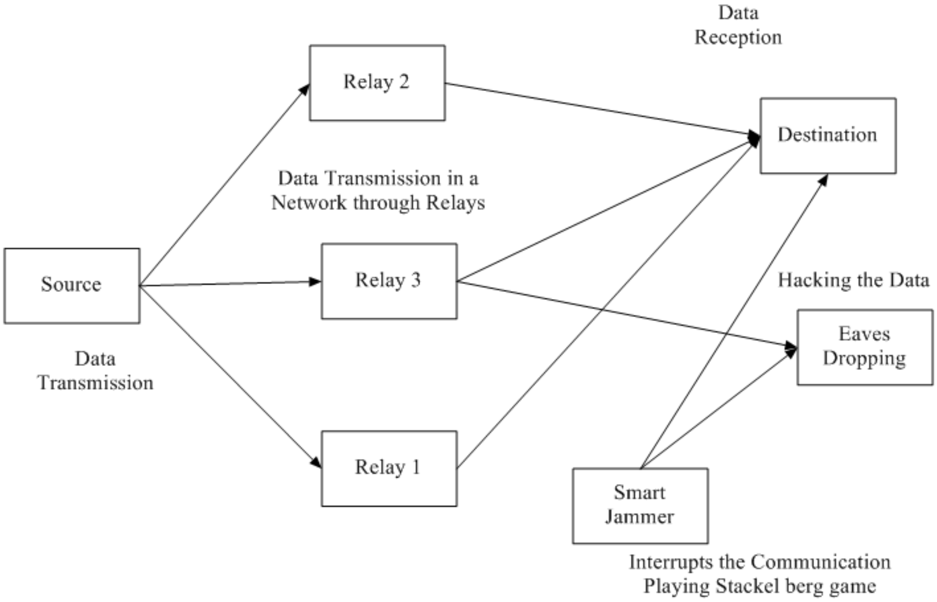
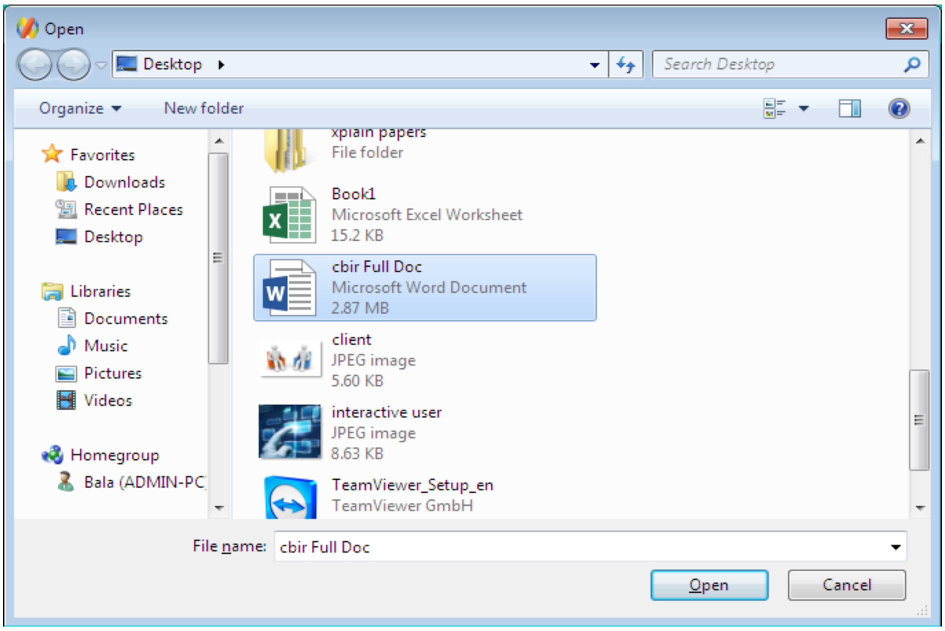
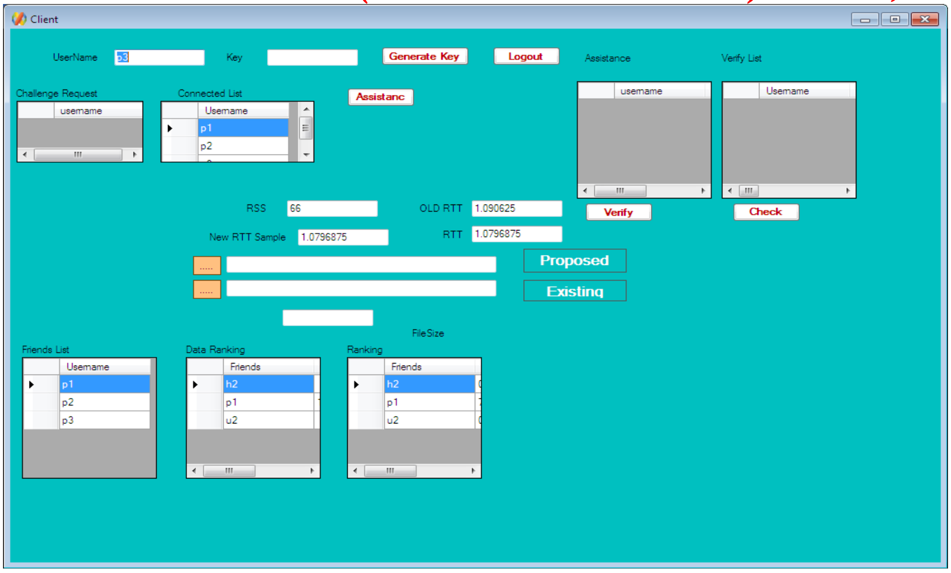


Figure 2: Jamming attack strategies and network defense in wireless sensor networks

**Browse the File:**



File name: cbir Full Doc



UserName p3
Key
RSS 66
OLD RTT 1.090625
New RTT Sample 1.0796875
RTT 1.0796875

| usename |
|---|

| Username |
|---|
| p1 |
| p2 |

| usemame |
|---|

| Usemame |
|---|

| Usemame |
|---|
| p1 |
| p2 |
| p3 |

| Friends |
|---|
| h2 |
| p1 |
| u2 |

| Friends |
|---|
| h2 |
| p1 |
| u2 |

## 4. Conclusion:

Here studied controllable jamming attacks in wireless sensor networks, which are easy to launch and difficult to detect and confront. The derived solutions to the optimization problems dictate optimal attack and network defense strategies. Of particular interest is the comparison between the case of perfect knowledge and that of lack of knowledge of the attacker and the network about the strategy of each other. In the latter, the attacker and the network respond optimally to the worst-case strategy of the other.

## 5. Future Work:

Another interesting issue is to find alternatives for modeling lack of knowledge for the attacker and the network. An idea would be to average over all strategies of the opponent. 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. Finally, the issue of multiple, potentially co-operating attackers gives a whole new flavor to these problems and is worth further attention.

## 6. References:

1. X. Shen, A. Hjrungnes, Q. Zhang, P. R. Kumar, and Z. Han, "Guest editorial: Cooperative networking - challenges and applications (Part 1)," IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 241–244, Feb. 2012.
2. B. Han, J. Li, J. Su, and J. Cao, "Self-supported cooperative networking for emergency services in multi-hop wireless networks," IEEE J. Sel. Areas Commun., vol. 30, no. 2, p. 450–457, Feb. 2012.
3. Y. Sun, W. Trappe, and K. J. R. Liu, Network-Aware Security for Group Communications. New York, NY, USA: Springer, 2007.
4. K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," IEEE Wireless Commun. Mag., vol. 18, no. 4, pp. 6–12, Aug. 2011.
5. Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in Proc. IEEE Conf. Comput. Commun., 2011, pp. 1422–1430.
6. Y. Liang, H. V. Poor, and S. Shamai, Information Theoretic Security. Delft, The Netherlands, Now Publishers, 2009.

7. Y. Liang, H. V. Poor, and L. Ying, "Wireless broadcast networks: Reliability, security, and stability," in Proc. IEEE Inf. Theory Appl. Workshop, Feb. 2008, pp. 249–255.
8. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.
9. S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, Jul. 1978.
10. Csiszar and J. Korner, "Broadcast channel with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.VI.