DETECTING MALICIOUS BEHAVIOR IN WIRELESS NETWORK USING KEY GENERATION ALGORITHM

Dr.M. Ramesh Kumar[1], Dr.S.R.Boselin Prabhu[2], D.Arthi[3], R.Sasikala[4], K.N.Jayapriya[5]
[1]Associate Professor, Department of Computer Science and Engineering,
VSB College of Engineering Technical Campus, Coimbatore, TamilNadu, India.
[2]Associate Professor, Department of Electronics and Communication Engineering,
VSB College of Engineering Technical Campus, Coimbatore, TamilNadu, India.
[3,4,5]Asst Professor, Department of Computer Science and Engineering,
VSB College of Engineering Technical Campus Coimbatore, TamilNadu, India.

ABSTRACT

Security of Wireless sensor network (WSN) becomes a very important issue that is vulnerable to a wide range of attacks due to deployment in the hostile environment and having limited resources. Intrusion detection system is one of the major and efficient defensive methods against attacks in WSN.In this paradigm, the intermediate nodes are responsible for relaying packets from the source to the destination. We develop Audit-based Misbehavior Detection system that effectively and efficiently isolates both continuous and selective packet droppers. When ad hoc networks are deployed in hostile environments (tactical networks), or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order to degrade the network performance. In this paper, we have to improve the security and performance. For this purpose, Encryption and decryption techniques are used with the help of key provider for providing the data security in the network.

Keywords: Hostile environment, Audit-Based.

1. INTRODUCTION

Intrusion detection is an important research topic with many potential applications. Along with intrusion prevention, response and tolerance, intrusion detection is one tool that can defend against the real-world cyber attacks threatening critical systems. These attacks include the Stuxnet attack on Iranian engineering facilities, proof of concept attacks on insulin pumps and cardiac devices, the DoS attack on a German power grid operator, the ex filtration attack on a Spanish power grid vendor and the ex filtration attack on MGCPSs (Mobile group cyber Physical System), MCPSs (Medical cyber Physical System) and UACPSs (Unmanned aircraft CPS) are critical wireless network systems because of their human impact. For a battalion of 25 firefighters, failure of their MGCPS can be fatal to the group or an individual. If the MGCPS does not identify a dangerous chemical in the environment and route that information correctly, the entire team is in jeopardy. For a hospital with 833 beds (e.g., Inova Fairfax Hospital), failure of their MCPS can be fatal to an individual. One of the primary functions of an MCPS is to administer analgesics. Overmedicating a patient will cause cardiac arrest. Another MCPS primary function is to provide cardiac support. Doing so when unnecessary or failing to do so when appropriate will kill the patient. In July 2012, 620 million customers in India lost power for up to two days. A combat vehicle belonging to a UACPS could use weapons against noncombatants. Malicious behavior damages the network by violating confidentiality, integrity, availability, authenticity, non-repudiation or privacy; for example, a node in a mobile telephony network masquerades as another node

in order to defeat the integrity of the billing function. Selfish behavior is a non-community minded action; for example, a node in a Mobile Ad Hoc Network (MANET) does not forward packets. We make this distinction because it is critical to consider the attack model when evaluating a defensive technique.

2. RELATED WORK

In “A Jamming-Resistant MAC Protocol for Multi-Hop Wireless Networks” a simple local medium access control protocol, called Jade, for multi-hop wireless networks with a single channel that is provably robust against adaptive adversarial jamming. The wireless network is modeled as a unit disk graph on a set of nodes distributed arbitrarily in the plane. In addition to these nodes, there are adversarial jammers that know the protocol and its entire history and that are allowed to jam the wireless channel at any node for an arbitrary (1 − _)-fraction of the time steps, where 0 < _ <1 is an arbitrary constant. We assume that the nodes cannot distinguish between jammed transmissions and collisions of regular messages. Nevertheless, we show that Jade achieves an asymptotically optimal throughput if there is a sufficiently dense distribution of nodes.

In “A Review of Anomaly based Intrusion Detection Systems” the advent of anomaly-based intrusion detection systems, many approaches and techniques have been developed to track novel attacks on the systems. High detection rate of 98% at a low alarm rate of 1% can be achieved by using these techniques. Though anomaly-based approaches are efficient, signature-based detection is preferred for mainstream implementation of intrusion detection systems. As a variety of anomaly detection techniques were suggested, it is difficult to compare the strengths, weaknesses of these methods. The reason why industries don’t favor the anomaly-based intrusion detection methods can be well understood by validating the efficiencies of the all the methods. To investigate this issue, the current state of the experiment practice in the field of anomaly-based intrusion detection is reviewed and survey recent studies in this. This paper contains summarization study and identification of the drawbacks of formerly surveyed works.

In “Trust-Based Routing and Intrusion Detection” we propose a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. Unlike prior work, we consider multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. By means of a novel probability model, we describe a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviors with the objective to yield “ground truth” node status. This serves as a basis for validating our protocol design by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of our hierarchical trust management protocol, we apply it to trust-based geographic routing and trust-based intrusion detection. For each application, we identify the best trust composition and formation to maximize application performance. Our results indicate that trust-based geographic routing approaches the ideal performance level achievable by flooding-based routing in message delivery ratio and message delay without incurring substantial message overhead. For trust-based intrusion detection, we discover that there exists an optimal trust threshold for minimizing false positives and false negatives. Furthermore, trust-based intrusion detection outperforms traditional anomaly-based intrusion detection approaches in both the detection probability and the false positive probability.

In “Anti-Jamming broadcast communication using uncoordinated frequency hopping“ proposes a technique called uncoordinated frequency hopping to counteract the jamming attack without using any shared keys. With the use of node cooperation this proposal achieves communication efficiency and stronger jamming resistance. In this network the nodes are acting as relay nodes i.e., it will broadcast the message to all nodes. This paper proposes collaborative broadcast protocol which analyses the successful packet reception rate and node cooperation. In these schemes the broadcast message is subdivided into multiple short packets and each packet is transmitted over a selected channel which is known to the sender. Such channel switching over a large frequency range effectively eliminates jamming attack. Further enhance the same in uncoordinated direct sequence spread spectrum, in which each transmitter sends the message with the help of spreading sequence randomly selects from a set. The receiver can retrieve the message only by choosing the same synchronized message chose by the transmitters. So the jamming effect eliminated with the use of UDSSS and collaborative protocol.

In "A New clustering approach for anomaly intrusion detection" have made our work easier compare to earlier times. Computer network is growing day by day but while discussing about the security of computers and networks it has always been a major concerns for organizations varying from smaller to larger enterprises. It is true that organizations are aware of the possible threats and attacks so they always prepare for the safer side but due to some loopholes attackers are able to make attacks. Intrusion detection is one of the major fields of research and researchers are trying to find new algorithms for detecting intrusions. Clustering techniques of data mining is an interested area of research for detecting possible intrusions and attacks. This paper presents a new clustering approach for anomaly intrusion detection by using the approach of K-medoids method of clustering and its certain modifications. The proposed algorithm is able to achieve high detection rate and overcomes the disadvantages of K-means algorithm.

3. MALICIOUS BEHAVIOR DETECTION

Earlier solutions for identifying misbehaving nodes either by using some form of per-packet evaluation of peer behavior or provide cooperation incentives to stimulate participation. Transmission overhearing becomes highly complex in multichannel networks or when nodes are equipped with directional antennas. On the other hand, per-packet behavior evaluation techniques are based on either transmission overhearing or issuance of per-packet acknowledgements. These monitoring operations must be repeated on every hop of a multi hop route, thus leading to high communication overhead and energy expenditure. Moreover, they fail to detect dropping attacks of selective nature, since intermediate monitoring nodes may not be aware of the desired selective dropping pattern to be detected.

3.1. Disadvantages

- Fail to detect dropping attacks of selective nature.
- It lead to high communication overhead and energy expenditure.

4. KEY GENERATION TECHNIQUE

To overcome these limitations, we propose a system called Audit-based Misbehavior Detection. To protect wireless sensor networks from the various weaknesses, preventive mechanisms like authentication and cryptography can be used to fend some type of attacks that are extruders. These type of methods or mechanisms define the primarily line of defense for the wireless sensor networks which achieves per-packet behavior evaluation without incurring a per-packet per-hop cost.

AMD is a comprehensive solution that integrates identification of misbehaving nodes, reputation management and discovery of trusted route in a distributed and resource-efficient manner.

4.1. Advantages

- It can operate in multi-channel networks and in networks with directional antennas.
- Detects selective dropping behaviors.
- Improving performance and data security.

5. DESCRIPTION OF THE TECHNIQUE

Wireless sensors networks (WSN) are planned in unattended surroundings in which energy replacement is difficult if not possible. Due to partial income, a WSN should not only assure the application specific QoS requirements such as timeliness, security, and reliability, but also reduce energy consumption to extend the system helpful lifetime.

The WSN aim is maximize the system lifetime exchange between the energy consumption vs. reliability. However, no previous work exists to consider the exchange in the presence of malicious attackers. It is commonly believed in the explore neighborhood that cluster is an effective solution for reach scalability, energy conservation, and reliability.

If use homogeneous nodes which rotate among themselves in the roles of cluster heads (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED for lifetime maximization has been consider. Demonstrated that using heterogeneous nodes can further improve performance and extend the system lifetime.

In the last case, nodes with greater resources provide as CHs performing computation all intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment.

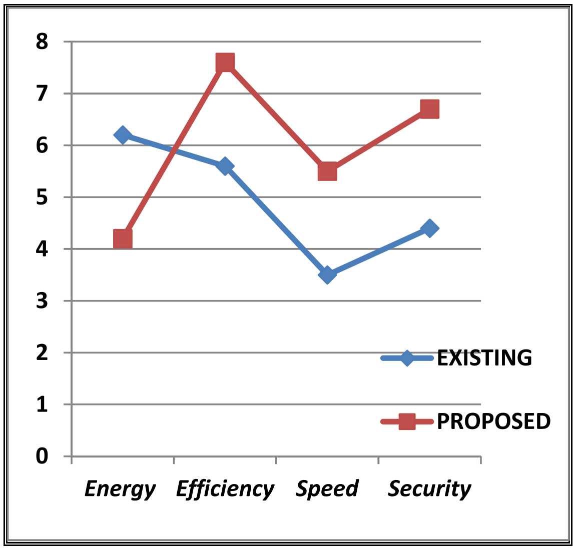

Figure.1 Comparison Between Existing and Proposed

In the absence of a supporting infrastructure, wireless ad hoc networks realize end-to-end communications in a cooperative manner. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range.

In this paradigm, intermediate nodes are responsible for relaying packets from the source to the destination. As an example, consider depicting a source S using a multi-hop path to route data to a destination D.

This network model presupposes that intermediate nodes are willing to carry traffic other than their own. When ad hoc networks are deployed in hostile environments (tactical networks), or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order to degrade the network performance.

Moreover, selfish users may misconfigure their devices to refuse forwarding traffic in order to conserve energy. This type of behavior is typically termed as node misbehaviors.

5.1 ***System Architecture***

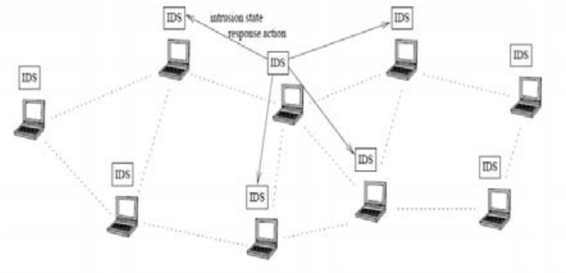

Figure.2 Nodes at the network

5.2 Node Signature Creation

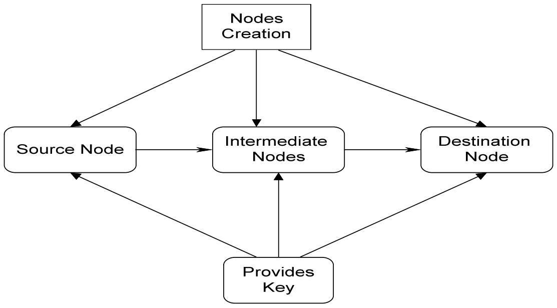

Figure.3 Creation of nodes and connections

In this module we create node for communication. Source node can send message through the intermediate node. We create GUI for each node and the help of the GUI we will communicate between source and destination node. The monitoring network server will maintain the node. We also form a network topology among the node. Each Node in the network has its own key and key is provided by key provider.

5.3Route Discovery

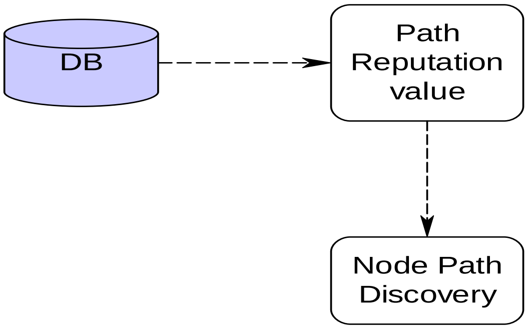

Figure.4 finding the trusted path from cache

The route discovery module is responsible for the discovery of trustworthy paths from a source to a destination (PSD). This module is invoked by the source whenever there is no cached path to the destination.

A path from source to destination can be seen as an in-series system of independent components. The failure of one component (a node dropping packets) results in the failure of the entire system. To discover trustworthy routes, we modify the discovery phase of the DSR protocol.

In DSR, when S has packets for D, it checks whether a route exists in its cache. If a route does not exist, S broadcasts a Route Request (RREQ) message. This Encrypted message contains the source ID, destination ID, and the time-to-live (TTL).

Any intermediate node that receives the RREQ appends its ID to the RREQ message and rebroadcasts it while decreasing the TTL field by one unit. If a receiving node is the destination, D responds to S with a route reply (RREP) message containing the entire PSD. The RREP follows the reverse path to S.

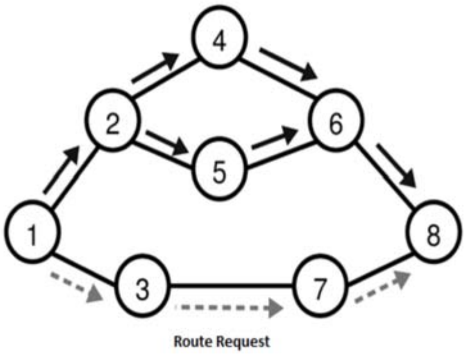

Figure.5 Route Request from source

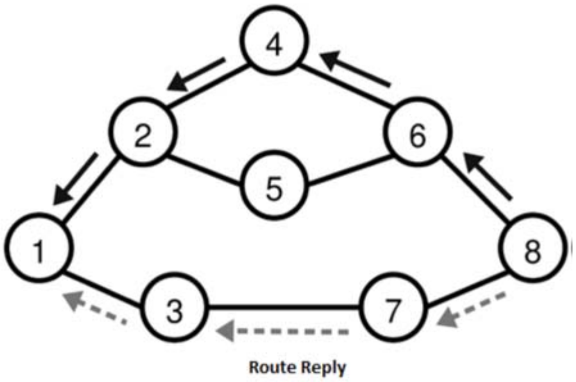

Figure.6 Route Reply from destination

5.4.Misbehaving Node Identification

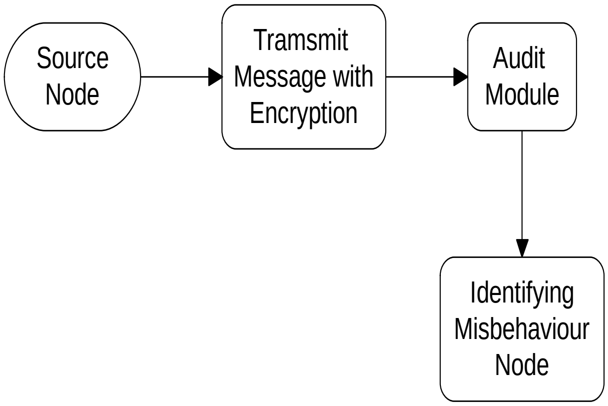
Source Node
Tramsmit Message with Encryption
Audit Module
Identifying Misbehaviour Node

Figure.7 Identification of Malicious Nodes

The audit module is responsible for identifying the set of nodes that misbehave in a particular path *PSD*. The source invokes the audit module if it detects poor performance on *PSD*.

The exact definition of what constitutes poor performance can be determined on the basis of a specific application running between *S* and *D*. Once the source has converged to a misbehaving link, it can no longer proceed to identify the misbehaving node.

5.5 Recover Packets

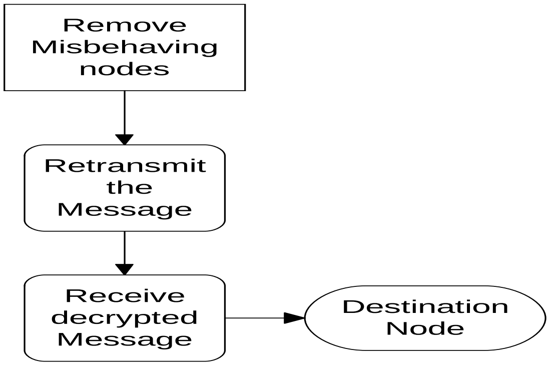

Figure.8 Recovery of packets by decryption

After removing misbehaving nodes, we have to transmit a message from S to D. In this Module, receiver received the packets from the nodes and convert into a file. The files are decrypted by applying the decryption algorithm. After complete these process stored the file in our preferred location.

6. ALGORITHM

6.1 Reputation-based Audit Algorithm

AMD (Audit based Misbehavior Detection) isolates misbehaving nodes by implementing a reputation based system. Nodes with low reputation values are excluded from routing paths, thus being unable to drop transit traffic. The reputation module is responsible for computing and managing the reputation of nodes. We adopt a decentralized approach in which each node maintains its own view of the reputation of other nodes. Such implementation alleviates the communication overhead for transmitting information to a centralized location, and readily translates to the distributed nature of ad hoc networks. Moreover, it allows nodes to hold individualized reputation metrics for their peers depending on their direct and indirect interactions. We take into account both *first-hand* and *second-hand* information. Information is considered to be first-hand if it is obtained by direct interaction between nodes (e.g., node *ni* routes information via node *nj*), and is considered to be second-hand if it is indirectly obtained based on the opinions of other nodes.

```
Initialize: $V = \{nl, . . . , nr\}, nl \leftarrow n1, nr \leftarrow nk$
while $|V| > 2$
{ $h \leftarrow$ argmin$V\ riS$
    audit($nh-1$)
    if $ah-1 = 0$
        $nr \leftarrow nh-1$
    else
    { audit($nh+1$)
        if $ah+1 = 1$
            $nl \leftarrow nh+1$
        else
        { audit($nh$)
            if $ah = 0$
                $nr \leftarrow nh$
            else
                $nl \leftarrow nh$ }}}
audit($nl, nr$)
if $al$ _= $ar$
    return $nl, nr$
else
    return $|M| \geq 2$, Partition PSD
```

6.2.Key Generation Algorithm

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms(such as RSA). Symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone (often by means of a digital certificate). A sender encrypts data with the public key; only the holder of the private key can decrypt this data. Since public-key algorithms tend to be much slower than symmetric-key algorithms, modern systems such as TLS and SSH use a combination of the two: one party receives the other's public key, and encrypts a small piece of data (either a symmetric key or some data used to generate it). The remainder of the conversation uses a (typically faster) symmetric-key algorithm for encryption. Computer cryptography uses integers for keys. In some cases keys are randomly generated using a random number generator (RNG) or pseudorandom number generator (PRNG). A PRNG is a computer algorithm that produces data that appears random under analysis. PRNGs that use system entropy to seed data generally produce better results, since this makes the initial conditions of the PRNG much more difficult for an attacker to guess. In other situations, the key is created using a passphrase and a key generation algorithm, usually involving a cryptographic hash function such as SHA-1.

7. THE NEED FOR INTRUSION DETECTION

Intrusion prevention measures, such as encryption and authentication, can be used in ad-hoc networks to reduce intrusions, but cannot eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes, which often carry the private keys. Integrity validation using redundant information (from different nodes), such as those being used in secure routing , also relies on the trust-worthiness of other nodes, which could likewise be a weak link for sophisticated attacks. Intrusion detection presents a second wall of defense and it is a necessity in any high-survivability network. In summary, mobile computing environment has inherent vulnerabilities that are not easily preventable. To secure mobile computing applications, we need to deploy intrusion detection and response techniques, and further research is necessary to adapt these techniques to the new environment, from their original applications in fixed wired network. In this paper, we focus on a particular type of mobile computing environment called mobile ad-hoc networks and propose a new model for intrusion detection and response for this environment.

8. CONCLUSION

We developed AMD, comprehensive misbehavior detection and mitigation system which integrates three critical functions: reputation management, route discovery, and identification of misbehaving nodes via behavioral audits. We modeled the process of identifying misbehaving nodes as R´enyi-Ulam games and derived resource-efficient identification strategies. We showed that AMD recovers the network operation even if a large fraction of nodes is misbehaving at a significantly lower communication cost. Moreover AMD can detect selective dropping attacks over end-to- end encrypted traffic streams.

9. FUTURE WORKS

Furthermore, we are providing security using cryptographic techniques with key generation algorithm. In this case, we improve the performance and security in wireless sensor network.

10. REFERENCES

[1]G. Alnifie and R. Simon. A multi-channel defence against jamming attacks in wireless sensor networks. In Proc. of Q2SWinet ’07, pages 95–104, 2007.

[2]B. Awerbuch, A. Richa, and C. Scheideler. A jamming-resistant MAC protocol for single-hop wireless networks. In Proc. of PODC ’08, 2008.

[3]E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa. On the performance of IEEE 802.11 under jamming. In Proc. of IEEE Infocom ’08, pages 1265–1273, 2008.

[4] M. A. Bender, M. Farach-Colton, S. He B. C. Kuszmaul, and C. E. Leiserson . Adversarial contention resolution for simple channels. In Proc. of SPAA ’05, 2005.

[5]T. Brown, J. James, and A. Sethi . Jamming and sensing of encrypted wireless adhoc networks. In Proc. of MobiHoc ’06, pages 120–130, 2006.

[6]J. Chiang and Y.-C. Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In Proc. of MobiCom ’07, pages 346–349, 2007.

[7]B. S. Chlebus , D. R. Kowalski, and M. A. Rokicki . Adversarial queuing on the multiple-access channel. In Proc. of PODC ’06, 2006.

[8]Czumaj and W. Rytter . Broadcasting algorithms in radio networks with un-known topology. Journal of Algorithms, 60(2):115 – 143, 2006.

[9]S. Dolev, S. Gilbert, R. Guerraoui, D. Kowalski, C. Newport, F. Kuhn, and N. Lynch. Reliable distributed computing on unreliable radio channels. In Proc2009 MobiHoc S3 Workshop, 2009.

[10]S. Dolev, S. Gilbert, R. Guerraoui, F. Kuhn, and C. C. Newport. The wireless synchronization problem. In Proc. 28th Annual ACM Symposium on Principles of Distributed Computing (PODC), pages 190–199, 2009.

[11]S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport. Gossiping in a multi-channel radio network: An oblivious approach to coping with malicious interference. In Proc. of the Symposium on Distributed Computing (DISC), 2007.

[12]S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport. Secure communication over radio channels. In Proc. 27th ACM Symposium on Principles of Distributed Computing (PODC), pages 105–114, 2008.

[13]S. Dolev, S. Gilbert, R. Guerraoui, and C. C. Newport. Gossiping in a multi-channel radio network. In Proc. 21st International Symposium on Distributed Computing (DISC), pages 208–222, 2007.

[14]S. Gilbert, R. Guerraoui, D. Kowalski, and C. Newport. Interference-resilient information exchange. In Proc. of the 28th Conference on Computer Communications. IEEE Infocom 2009., 2009.

[15]S. Gilbert, R. Guerraoui, D. R. Kowalski, and C. C. Newport. Interference-resilient information exchange. In Proc. 28th IEEE International Conference on Computer Communications (INFOCOM), pages 2249–2257, 2009.