An Effective Approach for Providing Anonymity in Wireless sensor Network: Detecting Attacks and Security Measures

Pooja Sharma Pawan Bhadana
B.S. Anangpuria Institute of Technology and Management Faridabad, Haryana

Abstract- **A wireless sensor network (WSN) consists of a large number of inexpensive and small nodes with sensing, data processing, and communication capabilities, which are densely deployed in a region of interest and collaborate to accomplish a common task. One main challenge in design of these networks is their vulnerability to security attacks. Security is becoming a major concern for WSN protocol designers. However, developed cryptography techniques are used, to detect, prevent or recover from security attacks . But the experience shows, there is cost involved with applying any security mechanism, which tends to be proportional to the amount of protection provided and has become major hindrances in security assessment of WSNs against posed attacks. This results in less reliable sensor networks and applications. In our strong opinion, there are two root-causes of this problem; 1) a comprehensive list of security attacks is overlooked and, 2) attacks are not associated with security frameworks. In this paper, we focus on taxonomy of attacks on wireless sensor networks comprehensively .We explore the security mechanism relevant to handle those attacks networks including key management, secure routing, intrusion detection , secure data aggregation secure group management .**

Keywords: **Wireless Sensor Network, Security, Vulnerabilities, Security Mechanism.**

1. INTRODUCTION

Advancements in integrated circuits have fostered the emergence of a new generation of tiny, inexpensive low-power sensors. WSN consists of small battery powered wireless devices (sensors) that are capable of monitoring environmental conditions such as humidity, temperature, noise, etc operating in an unattended mode. Sensor networks do not have a fixed infrastructure but form an ad hoc topology using wireless communication channels. With these types of devices there is a fundamental ability to share information. Sensor networks are characterized by dense node deployment, unreliable sensor node, frequent topology change, and severe power, computation and memory constraints because the nodes will often operate with finite battery resources. One main challenge in design of these networks is their vulnerability to security attacks.

Along with the explosive growth of computer networks in the last decades, the security of information transmitted over the networks has become an ever-increasing concern among the network users. It is well known that there are various attacks that threaten the confidentiality, integrity and availability of the information. We observe the problem of hiding the meta information of traffic pattern from the eavesdropper such as the source and destination network addresses, or the actual network route taken by the flow. It is very difficult to predict what the eavesdropper can or cannot observe.

Wireless network security is an active research area at the present. Researchers have proposed various schemes to enhance security of sensor networks These schemes cover a large spectrum of security issues, e.g., key management , secure routing , authentication, etc., most notably cryptography, to detect, prevent or recover from security attacks and to protect the information. Even with these mechanisms, the sensor nodes could be made non-operational by malicious attackers or physical break-down of the infrastructure. Sensor networks can also be subjected to various forms of intrusions and attacks. The motivation for attacking a sensor networks could be, for example, to gain an undeserved and exclusive access to the collected data. Wireless network security is an active research area at the present.

The rest of the paper is structured as follows. In section 2, we describes the architecture of wireless sensor network. In Section 3 we focus on design constraints for routing in wireless sensor networks. We then present taxonomy of attacks on wireless sensor networks comprehensively in Section 4. We explore the security mechanism relevant to handle those attacks networks including key management, Secure routing, Secure group management, intrusion detection, secure data aggregation in Section 5 and conclude this paper in Section 6.

2. ARCHITECTURE OF WIRELESS SENSOR NETWORK

Figure 1 demonstrates the network architecture .It is a three-layer hierarchical network architecture, which consists of three types of sensor nodes similar to the architecture utilized in [1]:

- Low-power “Sensor Nodes (SN)" with limited functionality;
- Higher-power “Forwarding Nodes (FN)" that forward the data obtained form sensor nodes to upper layer;
- “Access Points (AP)", or called “Base Stations (BS)”that route data between wireless networks and the wired infrastructure.

In contrast to sensor nodes in flat ad hoc sensor networks, sensor nodes in the lowest layer of this hierarchical network do not offer multi-hop routing capability to its neighbors. *Sensor Nodes* (SNs) can be application specific (e.g., temperature sensors, pressure sensors, video sensors, etc.).

They are deployed in groups (or clusters) at strategic locations for surveillance or monitoring applications and are controlled by a higher layer node, the *Forwarding Node* (FN). For each cluster of SNs, there is one FN, which serves as cluster head. The SNs are responsible for sending the collected data to the local FNs. An FN processes the data streams it receives from the SNs within the cluster. We assume the FNs are trustful and won't be compromised. We also assume the APs are trustful, otherwise the adversary can inject any data without been detected.

Each FN has two wireless interfaces, one communicates with lower layer nodes (SNs), which belong to its management, and the other connects to higher layer nodes – *Access Points* (APs). APs are located on the highest layer in a wireless network, and have both wireless and wired interfaces.

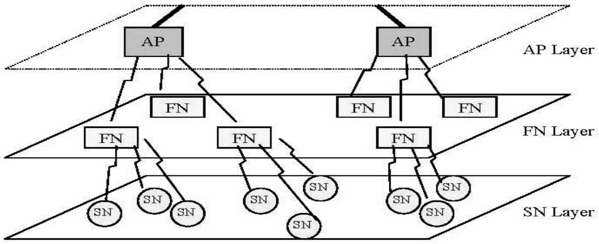

Fig 1. Architecture of hierarchical WSN.

APs provide multi-hop routing for packets from SNs and FNs within radio range, in addition to routing data to wired networks. APs also have the functionality of forwarding control information from wired networks to FNs and SNs. This hierarchical network can also be considered as a distributed information aggregation system. SNs gather information and report to its FN. Based on the information collected from SNs. FNs compute the aggregation result and commit the information to APs. However, since SNs may be compromised and report fake information, it is important for FNs to verify the correctness of the information collected from SNs. Similarly, it is also desired that APs possess the ability of verifying the committed information.

3. DESIGN CONSTRAINTS FOR ROUTING IN WIRELESS SENSOR NETWORKS

Due to the reduced computing, radio and battery resources of sensors, routing protocols in wireless sensor networks are expected to fulfill the following requirements:

a) Autonomy: The assumption of a dedicated unit that controls the radio and routing resources does not stand in wireless sensor networks as it could be an easy point of attack. Since there will not be any centralized entity to make the routing decision, the routing procedures are transferred to the network nodes.

b) Energy Efficiency: Routing protocols should prolong network lifetime while maintaining a good grade of connectivity to allow the communication between nodes. It is important to note that the battery replacement in the sensors is infeasible since most of the sensors are randomly placed. Under some circumstances, the sensors are not even reachable.

c) Scalability: Wireless sensor networks are composed of hundred of nodes so routing protocols should work with this amount of nodes. Any increase in network nodes should not affect the overall performance of the network.

d) Resilience: Sensors may unpredictably stop operating due to environmental reasons or to the battery consumption. Routing protocols should cope with this eventuality so when a current-in-use node fails, an alternative route could be discovered.

e) Device Heterogeneity: Although most of the civil applications of wireless sensor network rely on homogenous nodes, the introduction of different kinds of sensors could report significant benefits. The use of nodes with different processors, transceivers, power units or sensing components may improve the characteristics of the network. Among other, the scalability of the network, the energy drainage or the bandwidth are potential candidates to benefit from the heterogeneity of nodes.

f) Mobility Adaptability: The different applications of wireless sensor networks could demand nodes to cope with their own mobility, the mobility of the sink or the mobility of the event to sense. Routing protocols should render appropriate support for these movements.

4. TAXONOMY OF ATTACKS ON WIRELESS SENSOR NETWORKS

Absolute security is not practical. It is crucial to determine what security attacks an adversary can possibly conduct to compromise security. Here in this section, we present taxonomy of attacks on wireless sensor network.

4.1Passive attack vs. Active attacks

A passive attack is in the nature of eavesdropping on, or monitoring of, transmissions. The attacker tries not to interfere during the transmissions and attempts to be as "invisible" as possible. An active attack involves some modification of transmitted messages or the creation of fake messages. Active attacks can be detected by many means . Passive attacks and active attacks present the opposite characteristics. Passive attacks are very difficult to detect, because they do not involve any alteration of data, whereas active attacks can be detected by many means. Passive attacks can be prevented, to certain degree, whereas it is quite difficult to prevent active attacks. The adversary obtains flow information through passive attacks, i.e., eavesdropping conduct to compromise security.

4.2 Internal vs External Attacks

If an attacker launches attacks from compromised network nodes, it is called an internal attacker; and External attacks [6], [9] are defined as attacks from nodes, which do not belong to a WSN. Once a node is compromised, the attacker acquires its internal states and cryptographic secrets. So cryptographic method is useless against internal attacks.

4.3 Attacks on Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks on wireless sensor networks.

a) Spoofed, Altered, or Replayed Routing Information

This type of attack targets the routing information exchanged between nodes [5]. An attacker may spoof, alter, or replay routing information with the intention to disrupt the network traffic. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency which in turn causes increased traffic congestion and deprives the network of resources.

b) Selective forwarding

WSNs are usually multi-hop networks and hence based on the assumption that the participating nodes will forward the messages faithfully. Selective forwarding occurs when a compromised node drops a packet that is bound for a particular destination. In this way, an attacker can selectively filter traffic from a particular part of the network [5]. Other possible variations of selective forwarding can involve dropping all packets If all packets are dropped, then the attack is called a "black hole". Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow.

c) Blackhole /Sinkhole Attacks

In this attack, a malicious node acts as a blackhole [2] to attract all the traffic in the sensor network and can selectively suppress or modify packets originating from any node in the area. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes causing neighbouring nodes to assume that the compromised node is the best path to their destinations as shown in figure 2. Geo-routing protocols are known as one of the routing protocol classes that are resistant to sinkhole attacks, because that topology is constructed using only localized information, and traffic is naturally routed through the physical location of the sink node, which makes it difficult to lure it elsewhere to create a sinkhole.

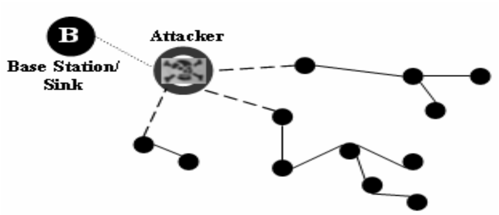

Fig 2: Sybil Attack

d) Sybil Attacks

In a Sybil attack, the malicious node gathers several identities for posing as a group of many nodes instead of a one[6] as shown in figure 3. This attack is not relevant as a routing attack only; it can be used against any crypto schemes that divide the trust between multiple parties. Resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [3].

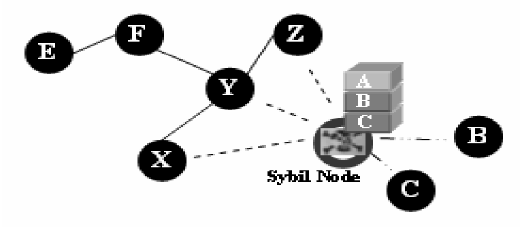

Fig 3: Conceptual view of Blackhole Attack

e) Acknowledgement Spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. An adversary can spoof link layer acknowledgments for ''overheard'' packets designed for neighboring nodes[5] or in other words these acknowledgements can be forged, so that other nodes believe a weak link to be strong or disabled nodes alive. This results in packets being lost when traveling along such links.

f) Wormhole Attacks

Wormhole attack [4] is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location into the network. The wormhole attack usually needs two malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. To overcome this, the traffic is routed to the base station along a path, which is always geographically shortest or use very tight time synchronization among the nodes, which is infeasible in practical environments.

g) HELLO *flood attack*

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false. An attacker with a high powered antenna can convince every node in the network that it is their neighbour. If the attacker also advertises a high quality route it can get every node to forward data to it. Nodes at a large distance from the attacker will be sending their messages into oblivion leaving the network in a state of confusion. This attack can also be thought of as a type of broadcast wormhole. Routing protocols dependant on localised information are extremely vulnerable to such attacks.

h) Denial of Service

Denial of Service (DoS) [7], [25] is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

5. SECURITY MECHANISM

Security is sometimes viewed as a standalone component of a system's architecture, where a separate module provides security. This separation is, however, usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security must pervade every aspect of system design. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level and low-level.

5.1. Low-Level Security Mechanism

Low-level security primitives for securing sensor networks includes,
1. Key establishment and trust setup
2. Secrecy and authentication
3. Privacy
4. Robustness to communication denial of service
5. Secure routing

1) Key establishment and trust setup.

When setting up a sensor network, one of the first requirements is to establish cryptographic keys for later use. As we know sensor devices have limited computational power, making public-key cryptography [12] primitives too expensive in terms of system overhead. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes. The simplest solution for key establishment is a networkwide shared key. It could be possible for the attacker to compromise a single node that would reveal the secret key and thus allow decryption of all network traffic. To overcome this problem is to use a single shared key to establish a set of link keys, one per pair of communicating nodes, and then erase the networkwide key after setting up the session keys. However, this variant of the key-establishment process does not allow addition of new nodes after initial deployment.

Bootstrapping keys using a trusted base station is another option. Here, each node needs to share only a single key with the base station and set up keys with other nodes through the base station. This approach makes the base station a single point of failure, but because there is only one base station, the network may incorporate tamper-resistant packaging for the base station, ameliorating the threat of physical attack. In the future, we expect to see research on better random-key predistribution schemes providing resilience to node compromise. Ultimately, we need a secure and efficient key-distribution mechanism allowing simple key establishment for large-scale sensor networks.

2) Secrecy and authentication.

Cryptography is the standard defense [14]measure that provide the protection against eavesdropping, injection, and modification of packets. For achieving a high degree of security we use end-to –end cryptography in point-to-point communication but it requires that keys be set up among all end points and be incompatible with passive participation and local broadcast. Link-layer cryptography with a network wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes might eavesdrop or alter messages. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment as compared to currently available network cryptographic approaches.

3) Privacy

Sensor networks have also thrust privacy concerns to the forefront. The most obvious risk is that ubiquitous sensor technology might allow ill intentioned individuals to deploy secret surveillance networks for spying on unaware victims. Therefore, an additional system requirement is that guidelines regarding fair information practices are built into the networks, in an attempt to protect privacy rights. To elaborate, content, identity and location privacy of the network need to remain intact for a system to be considered 'private'. Olariu et al [8] take a good stab at privacy issues by defining schemes that maintain the anonymity of the virtual infrastructure of a WSNs. This was coupled by randomising communications, such that the cluster structure and coordinate system remain concealed to outside observers. This area still remains vastly unexplored. Scenarios need to be explored where privacy is being exploited and solutions need to be devised to solve these issues.

4) Robustness to communication denial of service.

In WSN, the intention of the attacker is to disrupt the network traffic by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed. One standard defense against jamming employs spread-spectrum communication. The networked nature of sensor networks allows new, automated defenses against denial of service. When the jamming affects only a portion of the network, a jamming-resistant network could defeat the attack by detecting the jamming, mapping the affected region, then routing around the jammed area [16].Further progress in this area will hopefully allow for greater security against denial-of-service attacks.

5) Secure routing

One major challenge to secure routing in WSNs is that it is very easy for a single node to disrupt the entire routing protocol by simply disrupting the route discovery process. Papadimitratos and Haas propose a secure route discovery protocol that guarantees, subject to several conditions, that correct topological information will be obtained [17]. In this, the security relies on the MAC (message authentication code) and an accumulation of the node identities along the route traversed by a message. In so doing, a source can discover the sensor network topology as each node along the route from source to destination appends its identity to the message. In order to ensure that the message has not been tampered with, a MAC is constructed and can be verified both at the destination and the source (for the return message from the destination). Mun and Shin [19], who suggest countermeasures for routing attacks that establish trust relationships between nodes and authenticate sent packets whilst checking node bi-directionality.

5.2. High-Level Security Mechanism

Now here, we consider high-level security mechanisms, including secure group management, intrusion detection, and secure data aggregation.

1) Secure Group Management

Since sensor nodes are required to group themselves in order to fulfill a particular task, it is necessary that the group members communicate securing between each other, despite the fact that global security may also be in use. In other words, the processing of the raw data consists of dividing the network into small groups and analyzing the data aggregated by the group leaders. So the group leader has to authenticate the data it is receiving from other nodes in the group. This requires group key management. However, addition or deletion of nodes from the group leads to more problems. Consequently, secure protocols for group management are required [21].Secure grouping has not been intensively researched in the past and only a few resource intensive solutions exist.

2) Intrusion detection

Typically a wireless sensor network uses cryptography to secure itself against unauthorized external nodes gaining entry into the network. But cryptography can only protect the network against the external nodes and does little to thwart malicious node who already possess one or more keys. An Intrusion Detection System (IDS) monitors a host or network for suspicious activity patterns outside normal and expected behavior .Brutch and Ko [15] have surveyed the challenges in intrusion detection and have proposed watchdog, control messages, neighbourhood watch and anomaly detection as possible solutions to dynamic source routing attacks. Since it is impossible for every node to have a full powered IDS agent due to resource limitations, the basic problem in this area is how to distribute the intrusion detection agents and their tasks in the network. Anjum et al [18] have used graph theory in order to optimally place the intrusion detection modules around the sensor network. Agah et al [10] proved that game theory techniques [20] can be applied as a defense technique which will outperform intrusion detection techniques based on intuitive metrics i.e. traffic loads and Markov decision processes.

Su et al [11] have researched how to apply intrusion detection techniques in cluster based networks, by making nodes aware of packet forwarding misbehaviour of their neighbours and by collectively monitoring the cluster heads. Finally, Kreibich and Crowroft [13] have described a system for automating attack signature generation that eliminates the costly procedure of audit data analysis on wired networks. Interesting results in terms of energy efficiency and detection accuracy may well be produced by combining some of the above aforementioned techniques into hybrid entities.

3) Secure Data Aggregation

Data aggregation (or “fusion”) is necessary in sensor networks to reduce the amount of data transmitted to the base station. This is possible because a sensor network is data centric [25].It could be possible for attacker to control over an aggregating node, injecting the false reports or ignore reports affecting the credibility of the generated data and hence the network as a whole. The main aim in this area is to use resilient functions, that will be able to discover and report forged reports through demonstrating the authenticity of the data somehow.

Wagner [22], established a technique in which the aggregator uses Merkle hash trees to create proof of its neighbours’ data, which in turn is used to verify the purity of the collected data to the base station. An other approach [23], takes advantage of the network density by using the aggregator’s neighbours as witnesses. It is also possible to reduce the amount of traffic heading to the base station by using bloom filters to filter out the false aggregations [24]. Improvements still need to be made in this area, such as minimizing the amount of negotiation data generated by interactive algorithms.

6. CONCLUSION

Wireless networking goes beyond the reach of computer networks, leading to the prospect of “anywhere and anytime” communication. The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes taxonomy of attacks on wireless sensor networks comprehensively .We explore the security issues relevant to handle those attacks networks including key management, secure routing, intrusion detection , secure data aggregation secure group management n and challenges for next generation WSNs and discuss the crucial parameters that require extensive investigations. This research will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

REFERENCES

[1] S. Zhao, K. Tepe, I. Seskar and D. Raychaudhuri, “Routing Protocols for Self-Organizing Hierarchical Ad-Hoc Wireless Networks,” *Proceedings of the IEEE Sarnoff Symposium*, Trenton, NJ, March 2003.

[2] Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSR MANETs”, Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[3] Newsome, J., Shi, E., Song, D, and Perrig, A, “The Sybil attack in sensor networks: analysis & defences”, Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[4] Hu, Y.-C., Perrig, A., and Johnson, D.B., “Packet leashes: a defense against wormhole attacks in wireless networks”, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[5] Karlof, C., & Wagner,. D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks Journal: Special Issue on Sensor Network Applications and Protocols.Vol.1,*

(p293-315), Elsevier Publications

[6] E. Shi and A. Perrig, “Designing Secure Sensor Networks,” Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[7] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., “Analyzing interaction between distributed denial of service attacks and mitigation technologies”, Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[8] S. Olariu, Q. Xu, M. Eltoweissy, A. Wadaa, and A. Y. Zomaya, “Protecting the communication structure in sensor networks,” International Jounral of Distribted Sensor Networks, vol. 1, pp. 187–203, 2005.

[9] Yong Wang, Garhan Attebury, and Byrav Ramamurthy, “A Survey Of Security Issues In Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.

[10] A. Agah, S. K. Das, K. Basu, and M. Asadi, “Intrusion detection in sensor networks: A non-cooperative game approach,” in Proceedings - Third IEEE International Symposium on Network Computing and Applications, NCA 2004, Aug 30- Sep 1 2004, Proceedings - Third IEEE International Symposium on Network Computing and Applications, NCA 2004, (Cambridge, MA, United States), pp. 343–346, IEEE Computer Society, Los Alamitos, CA 90720-1314, United States, 2004.

[11] C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.-F. Horng, “The new intrusion prevention and detection approaches for clustering-based sensor networks,” in 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005: Broadband Wireless for the Masses - Ready for Take-off, Mar 13-17 2005.

[12] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, “Security in wireless sensor networks: issues and challenges” Advanced Communication Technology (ICACT), Page(s):6, year 2006

[13] H. Han, X. L. Lu, J. Lu, C. Bo, and R. L. Yong, “Data mining aided signature discovery in network-based intrusion detection system,” Operating Systems Review (ACM), vol. 36, no. 4, pp. 7–13, 2002.

[14] D. Djenouri, L. Khelladi, and N. Badache, “A Survey of Security Issues in Mobile ad hoc and Sensor Networks,” *IEEE Commun. Surveys Tutorials*, vol. 7, pp. 2–28, year 2005.

[15] P. Brutch and C. Ko, “Challenges in intrusion detection for wireless ad-hoc networks,” in Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on, pp. 368–373, 2003.

[16] Wood, A., Stankovic, J., and Son, S. JAM: A mapping service for jammed regions in sensor networks. In *Proceedings of the IEEE Real-Time Systems Symposium* (Cancun, Mexico, Dec. 3–5, 2003).

[17] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2002), 2002.

[18] F. Anjum, D. Subhadrabandhu, and S. Sarkar, “Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols,” in 2003 IEEE 58th Vehicular Technology Conference, VTC2003-Fall, Oct 6-9 2003, vol. 58 of IEEE Vehicular Technology Conference, (Orlando, FL, United States), pp. 2152–2156, Institute of Electrical and Electronics Engineers Inc., Piscataway, United States, 2004.

[19] Y. Mun and C. Shin, “Secure routing in sensor networks: Security problem analysis and countermeasures,” in International Conference on Computational Science and Its Applications - ICCSA 2005, May 9-12 2005, vol. 3480 of Lecture Notes in Computer Science, (Singapore), pp. 459–467, Springer Verlag, Heidelberg, D-69121, Germany, 2005.

[20] M. Kodialam and T. Lakshman, “Detecting network intrusions via sampling: a game theoretic approach,” in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, vol. 3, pp. 1880–1889 vol.3, 2003.

[21] Mohit Saxena, “Security In Wireless Sensor Networks - A Layer Based Classification”, Cerias Tech Report 2007-04.

[22] D. Wagner, “Resilient aggregation in sensor networks,” SASN’04 – Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 78 – 87, 2004. Data aggregation;Sensor networks;Node capture attacks;Multi-party computation;Robust statistics;Average;Mean;Median;.

[23] W. Du, Y. S. Han, J. Deng, and P. K. Varshney, “A pair wise key pre-distribution scheme for wireless sensor networks,” Proceedings of the ACM Conference on Computer and Communications Security, pp. 42 – 51, 2003. Wireless sensor networks (WSN); Key pre-distribution; Network resilience; Ultra-small autonomous devices;.

[24] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” Proceedings - IEEE INFOCOM, vol. 4, pp. 2446 – 2457, 2004. Sensor networks’-route filtering mechanism (SEF); Authentication;.

[25] Wang, B-T. and Schulzrinne, H., “An IP traceback mechanism for reflective DoS attacks”, Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.