Wireless Sensor Network Security

Saurabh Sharma[1], Amit Sahu[2], Ashok Verma[3], and Neeraj Shukla[4]

[1] Computer Science Engineering
Gyan Ganga Institute of Technology & Sciences,
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Madhya Pradesh
[2] Computer Technology & Application
Gyan Ganga College of Technology,
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Madhya Pradesh
[3] Dept. Computer Science Engineering
Gyan Ganga Institute of Technology & Sciences,
Jabalpur, Madhya Pradesh
[4] Computer Technology & Application
Gyan Ganga College of Technology
Jabalpur, Madhya Pradesh
{saurabh.sharma44,kumaramitsahu,neerajshukla28}@gmail.com
ashokverma@ggits.org

Abstract. If sensor networks are to attain their potential, security is one of the most important aspects to be taken care of. The need for security in military applications is obvious, but even more benign uses, such as home health monitoring, habitat monitoring and sub-surface exploration require confidentiality. WSNs are perfect for detecting environmental, biological, or chemical threats over large scale areas, but maliciously induced false alarms could completely negate value of the system. The widespread deployment of sensor networks is directly related to their security strength. These stated facts form the basis for this survey paper. This paper present a brief overview of challenges in designing a security mechanism for WSN, classify different types of attacks and lists available protocols, while laying outline for proposed work.

Keywords: Wireless Sensor Networks, Security Protocols, Network Threats.

1 Introduction

Our previous work pertaining to use of Wireless Sensors in Subsurface exploration proposed novel and efficient deployment strategy [1], routing strategy [2], and information processing using Extended Kalman Filter [3]. Sensor network proponents predict a future in which numerous tiny sensor devices will be used in almost every aspect of life. The goal is to create smart environments capable of collecting massive amounts of information, recognizing significant events automatically, and responding appropriately. Sensor networks facilitate comprehensive, real-time data processing in complex environments. Typical applications of sensors include emergency response information, energy management, medical monitoring, inventory control, and

N. Meghanathan et al. (Eds.): CCSIT 2012, Part III, LNICST 86, pp. 317–326, 2012.

battle-field management. For potential use of sensor networks, secure communication techniques are required so that the system and its users get protected [4].

The need for security in military applications is obvious, but even more benign uses, such as home health monitoring, and sub-surface exploration require confidentiality. WSNs are perfect for detecting environmental, chemical, or biological threats over large scale areas, but maliciously induced false alarms are capable of negating value of the system. Widespread deployment of sensor networks is directly related to their security strength. These stated facts form the basis for this survey paper. Structure of the paper is as follows: Section 2 presents background and throws light on the work of researchers who proposed in-network security mechanisms. Section 3 presents attacks and defenses within WSN, while Section 4 outlines Sensor Security Challenges. Section 5 presents conclusion and proposed future work.

2 Related Work

Re-searchers of WSN have been concentrating on solving a variety of challenges ranging from limited resource capabilities to secure communication. Literature indicates that sensor networks are deployed in public or abandoned areas, over insecure wireless channels [5], [6], [7]. It is therefore alluring for a malicious device / intruder to eavesdrop or inject messages into the network. The traditional solution to this problem has been to take up techniques such as message authentication codes, public key cryptography and symmetric key encryption schemes. However, since there are resource scarcities for motes, the major challenge is to devise these encryption techniques in an efficient way without sacrificing their scarce resources. One method of shielding any network against external attacks is to apply a straightforward key infrastructure. However, it is known that global keys do not provide network resilience and pair wise keys are not robust solution. A more intuitive solution is needed for WSNs.

TinySec [8] introduced security to the link layer of TinyOS suite [9] by incorporating software-based symmetric keying with low operating cost requirements. Not all vulnerabilities present in TinySec could be addressed for example techniques to avoid insider attacks. In contrast, Zigbee or the 802.15.4 standard introduced hardware-based symmetric keying with success. The public key cryptography had been tested out in all development phases to provide complete security . This concept has opened an unheard area for discussion of sensor network cryptographic infrastructure. Wide-spread research is also being carried out on topics such as key storage & key sharing [10], key preservation [11] and shared key pools [12]. Now, since sensor nodes need to cluster aiming to fulfill a particular task, it is desired that the group members' converse securing between each other, in spite of the actuality of global security also present. But contrary to this fact secure grouping has been researched to a very low extent in the past and only a few exhaustive solutions exist.

Further, although, data aggregation (sensor nodes aggregate sensed data from environment before finally transmitting it to the base station) is one of the promising strategies to reduce cost and network traffic but such data is always susceptible to attacks by

intruders. A challenger with control over an aggregating node can choose to disregard reports or produce fake reports, affecting reliability of the generated data and at times whole network as well. The main aim in this area is to use flexible functions, which will be able to discover and report forged reports through demonstrating authenticity of the data somehow. Some technique had been established in which aggregator uses hash trees to create proof of its neighbors' data, which in turn is used to verify purity of collected data to the base station. Another approach [13], takes advantage of network density by using the aggregator's neighbors as witnesses. It is also possible to reduce amount of traffic heading to base station by using bloom filters to filter out false aggregations. Latest research trends towards security measures indicate development of Secure Protocols. The main research challenge in this area is to discover new defense techniques to be applied to existing routing protocols, without compromising connectivity, coverage or scalability [14]. Security Protocols in Sensor Networks (SPINS) provide data authentication, semantic security and low overhead, along with replay protection.

Fig 1 elaborates the energy cost of adding security protocols to sensor network. Majority of overhead arises from transmission of extra data rather than any computational costs. SPINS was later used to design a secure cluster based protocols such as LEACH. Karlof and Wagner [5] have provided an extensive analysis on the WSNs routing vulnerabilities and possible countermeasures. According to their study common sensor network protocols are generally vulnerable due to their simplicity and hence security should be incorporated into these protocols right from design time.

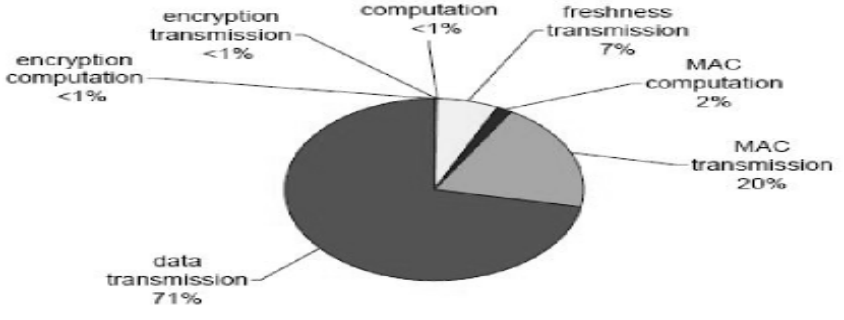

Fig. 1. Energy costs from SPINS [20]

3 Attacks and Defenses

Goals for security sensor networks include the same four primary objectives as conventional networks: availability, secrecy, integrity, and authentication. Though WSN security is characterized by the same properties as compared to traditional network security, but at the same time they are prone to new attacks. Attacks are made at several levels on the network, like Physical Layer, Link Layer or Network Layer.

Attacks at physical level include radio signal jamming as well as tampering with physical devices. One of the most prominent attacks at this layer is Jamming [15], a

well-known attack on wireless communication. In jamming, intruder interferes with wireless frequencies on which the transceivers used by a device operates. It represents an attack on the network accessibility. Jamming is different from normal radio transmission in that it is redundant and disorderly, thus creating a denial-of-service condition. The degree of jamming is determined by physical properties such as available power, antenna design, obstacles, and height above ground. Jamming is extremely successful against single channel networks, i.e., when all nodes transmits in small band, single wireless spectrum.

Tampering [16] is the second security issue at physical layer. Sensor nodes are generally deployed in hostile environment, away from personal monitoring. These sensors are available for easy access to intruders, which can potentially harm these devices by tampering, duplicating or even destroying them. One available solution to this problem is manufacturing of tamper-proof sensor nodes. These nodes are smart enough to delete any cryptographic information available within them as soon as they sense some sort of tampering. But these are not economically viable since tamper-proof sensor nodes increase overall cost. Other solutions might be using of multi-key security algorithms. In these security algorithms intruders will not have access to complete data even if one of the key has been compromised upon.

Like the physical layer, link layer is particularly vulnerable to denial of service attacks. The link and media access control (MAC) layer handles neighbor-to-neighbor communication and channel arbitration. The first type of attack at this layer is known as Collision. If a challenger is able to generate a collision of even part of a transmission, one can interrupt the entire packet. A single bit error will cause a Cyclic Redundancy Check (CRC) variance and would require retransmission. In some media access control protocols, a corrupted ACK (acknowledgment) may cause exponential back-off and pointlessly increase latency. Although error-correcting codes guard against some level of packet corruption, intentional corruption can occur at levels which are beyond the encoding scheme's capability to correct. The advantage, to the challenger, of this jamming at MAC level over physical layer jamming is that much less energy is required to achieve the same effect.

Another malicious goal of intruders is Exhaustion [17] of a sensor node's battery power resources. Exhaustion may be initiated by an interrogation attack. A compromised sensor node could repeatedly transmit RTS (Request To Send) packets in order to bring forth CTS (Clear To Send) packets from a uncompromised neighbor, eventually draining the battery power of both nodes. Still more damaging attack on Link Layer is Unfairness. In this type of attack at Link Layer, a compromised node can be misrepresented to sporadically attack the network in such a fashion which induces biasness in the priori-ties for granting of medium access. This fragile form of denial of service attack might, increase latency resulting in real-time protocols miss their deadlines. Another form of this attack generally target one particular flow of data in order to restrain recognition of some event. The use of tokens which avert a compromised node from capturing the channel for a long period of time has been proposed.

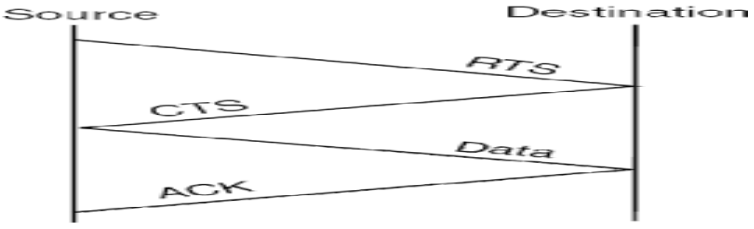

Fig. 2. A Four-Way Handshake ensures collision avoidance in 802.11 networks

Due to the ad-hoc nature of sensor networks, each node eventually at some point of time assumes routing responsibilities. Since every node in a sensor network virtually enact as a router, hence WSN are highly susceptible to routing attacks at network layer. Researchers have identified a variety of routing attacks and have shown them to be effective against major sensor network routing protocol. Various classifications of attacks are summarized below and followed by a general discussion of secure routing techniques.

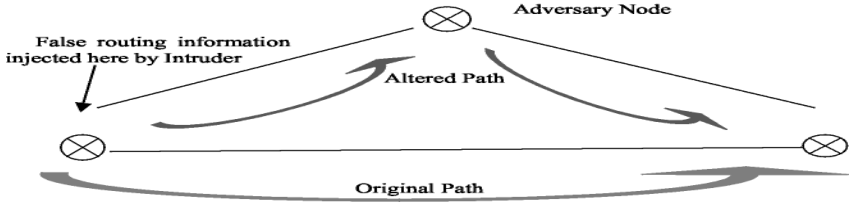

Fig. 3. Redirecting traffic through an adversary node via False Routing Information attack

The most prominent attack on routing is to alter, spoof, or just replay routing information. This type of attack is known as False Routing Information. The false information may allow intruder to attract or repel traffic, create routing loops, shorten or ex-tend route lengths, increase latency, and even partition the network, as shown in Fig 3. Clearly, the distortion of routing information can cripple complete network. The standard solution is to require authentication for routing information, i.e., routers only accept routing information from valid routers encrypted with valid shared key information.

Another attack, known as Selective Forwarding is a more clever attack in which the compromised node is made to transmit forward only some of the packets correctly, while others are silently dropped. Smart networks are capable to routing data along another path, in case of a failure of a particular node. If all packets from a node are dropped, it will be considered as a dead network. Hence only selective packets are being forwarded by compromised node, creating an illusion that it is still active, and that data can be routed via it.

Routing decisions in network are based on distance between nodes. In Sinkhole Attack a compromised node is made to advertise a luring route to the base station or sink. Thus all neighboring nodes are made to route their data towards the compromised node,

as shown in Fig 4. The intruder at compromised node thus gains access to major data within its area, and might destroy, manipulate or even modify these packets.

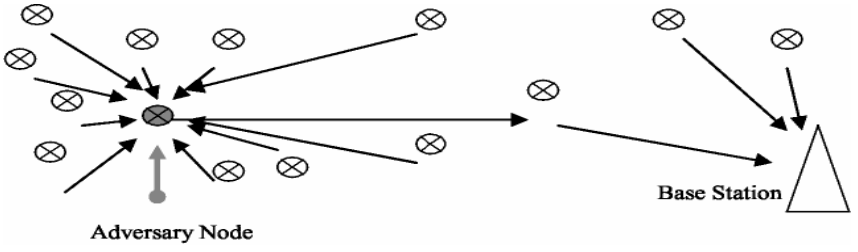

Fig. 4. Model of Sinkhole attack

In Sybil attack , the compromised node spoof neighboring nodes by broadcasting multiple identities. The compromised node claims to be other node present within the network, hence presenting a great threat to overall routing process [Fig 5]. The malicious effect aggravates as other nodes unknowingly further transmit routing data received from compromised node to their neighbors.

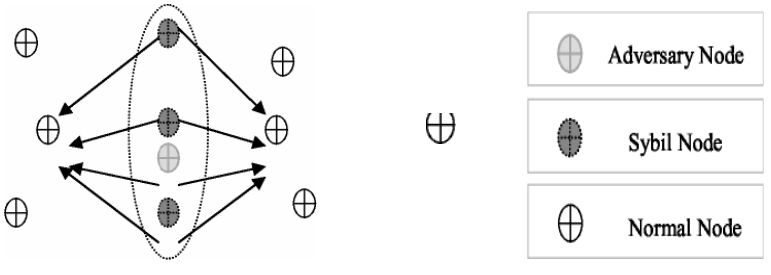

Fig. 5. Model of Sybil attack

In Wormhole Attack [18], two mutually understanding malicious nodes form an out-of-bound channel or transmission tunnel in between them. The end points of this tunnel are called as Start & End point. The compromised node at Start point transmits its data via tunnel to malicious node present at End point, as shown in Fig 6. The End point node then re-transmits the received data packets, hence creating an illusion that these distant nodes are neighbors. This sort of attack is likely to be used in arrangement with selective forwarding or eavesdropping.

Nodes present within a network rely on acknowledgment received from neighboring nodes. In Acknowledgment Spoofing attack [19], a malicious node may respond back to a transmitting node on behest of a weak or a non-active node, and thus deceiving sensor about strength of link. This way sender unknowingly keeps on transmitting to the non-active node and data is eventually lost or captured and destroyed by malicious node. There have been several approaches to defend against network layer attacks. Authentication and encryption may be initial steps, but more proactive techniques such

as monitoring, probing, and transmitting redundant packets have also been suggested. Secure routing methods protect against some of previous attacks. Proposed techniques include Authentication & Encryption. Link layer authentication and encryption protect against most outsider attacks on sensor network routing protocol. Even a simple scheme which uses a globally shared key will prevent unauthorized nodes from joining topology of the network. In addition to preventing selective forwarding and sinkhole attacks, authentication and encryption make Sybil attack almost impossible because nodes will not accept even one identity from the malicious node.

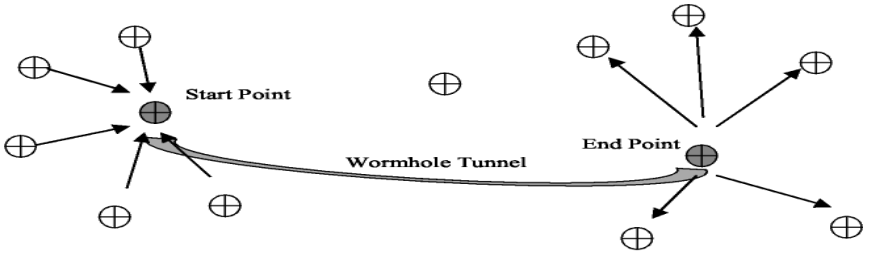

Fig. 6. Model of Wormhole Attack

Another technique is Monitoring, which is a more active strategy for secure routing, where-in nodes monitor their peers and watch for suspicious behavior. In this approach, motes act as "watchdogs" to monitor next hop transmission of the packet. In event that misbehavior is detected, nodes will update routing information in order to avoid the compromised node. Another proactive defense against malicious routers is probing. This method periodically sends probing packets across the network to detect blackout regions. Since geographic routing protocols have knowledge of the physical topology of the network, probing is especially well-suited to their use. Probes must appear to be normal traffic, however, so that compromised nodes do not intentionally route them correctly in order to escape detection. Redundancy is another strategy for secure routing. Redundancy simply transmits a packet multiple times over different routes. Hopefully one of the routes remains uncompromised and will correctly deliver message to the destination. Despite its inefficiency, this method does increase the difficulty for an attacker to stop a data flow.

4 Challenges in Sensor Security

Five of the most looked for challenges in designing security schemes for large wireless sensor networks are Wireless Medium, Ad-Hoc Deployment, Hostile Surroundings, Resource Scarcity and Immense Scale. The deployment scenarios for ad-hoc sensor motes renders use of wired media communication totally infeasible [20]. This leads to more security concerns in WSN, since wireless medium is always prone to security attacks since its method of operation / transmission makes it an easy prey for eavesdropping. Wireless communication can be easily trapped, modified or even replaced by

intruders. The wireless media allows intruders to destroy genuine communication packets and inject deceptive data into network, with least of the efforts. Wireless media security problem has been intrinsic to traditional networks too, but enhanced and robust solutions are required for sensor networks, owing to their unpredictable deployment and ad-hoc arrangement.

Another challenge for WSN security is its ad-hoc deployment. Sensors may be required to deploy in deterministic or non-deterministic environments. In both cases no fixed topology can be framed in advance. Even the deployed network may have to change its topology every now and then, subject to addition of new nodes, node failures etc. [21]. Under such conditions, robust security protocols are required which can adapt dynamically as per changing configuration / topology of WSN. Hence in sensor networks traditional security mechanisms based on static configurations cannot be applied.

The environment within which sensor nodes operate, collect and transmit data is hostile. Intruders might have know-about the geographical locations of sensor motes, and subsequently reach them to capture / destroy them. No security protocol can fend WSN against such kind of physical attacks, but these needs to be kept in scenario while designing a security framework, in order to provide self-healing capabilities to network.

Another challenge in WSN is resource scarcity within sensor motes. Due to hostile conditions and non-predictable environment sensor nodes cannot be replenished in terms of battery power. In addition to battery, the memory size and computational powers too are low due to small size of nodes. These factors make efficient but resource extensive security mechanisms totally infeasible for WSN. A representative example of sensor device is Mica mote. It has a 4 MHz Atmel ATMEGA103 CPU with 128 KB of instruction memory, 512 KB of flash memory, and just 4 KB of RAM for data. The radio operates at up to 40 Kbps bandwidth with a transmission range of a few dozen meters. Such constraints on resources demand extremely competent security algorithms in terms of computational complexity, memory as well as bandwidth. While energy is perhaps the most prized resource for sensor networks, earlier research work has given little to no attention to energy efficiency. Transmission is especially expensive in terms of power, as apparent from SPINS [Fig 1] too. The large scale deployment of WSN is its biggest confront. For small area application of WSN there are threats like Sinkhole attack have been overcomed [22]. Traditional networks might be limited to an office or to a bigger geographical location but in a controlled fashion. But in case of sensors, the area being covered may be large and un-predictable. In many cases sensors are even air-dropped and hence their exact geographical location may be different than what might have been thought of. In such cases providing security to all nodes present becomes a challenging task. The develpoment over such Security mechanism which can make available to large number of nodes spread over a large area, and at the same instance maintaining computational and communication efficiency.

5 Conclusion and Future Work

The paper presented known threats and security protocols available for wired and wire-less networks. Works of researchers in this field have been extensively studied. While many frameworks have been devised for WSN, but none were found for robust security mechanisms in subsurface exploration. Keeping in view the extreme harsh conditions prevailing in subsurface, the demand is to devise a novel security mechanism which will make communication within sensors more robust, scalable and efficient.

References

1. Juneja, D., Sharma, A., Kumar, A.: A Novel and Efficient Algorithm for Deploying Mobile Sensors in Subsurface. Computer and Information Science 3(2), 94–105 (2010) ISSN 1913-8989 (Print), ISSN 1913-8997 (Online)
2. Juneja, D., Sharma, A., Kumar, A.: A Query Driven Routing Protocol for Wireless Sensor Nodes in Subsurface. International Journal of Engineering Science and Technology 2(6), 1836–1843, ISSN: 0975-5462
3. Juneja, D., Sharma, A., Kumar, A.: A Novel Application Of Extended Kalman Filter For Efficient Information Processing In Subsurfaces. International Journal of Computer Applications 17(2), 28–32 (2011) ISSN: 0975-8887
4. Pathan, A.-S.K., Lee, H.-W., Hong, C.S.: Security in Wireless Sensor Networks: Issues and Challenges. In: ICACT 2006 (2006)
5. Lu, B., Habetler, T.G., Harley, R.G., Gutiérrez, J.A.: Applying Wireless Sensor Networks in Industrial Plant Energy Management Systems – Part I: A Closed-Loop Scheme. In: Sensors, October 30-November 3, pp. 145–150. IEEE, Los Alamitos (2005)
6. Bokareva, T., Hu, W., Kanhere, S., Ristic, B., Gordon, N., Bessell, T., Rutten, M., Jha, S.: Wireless Sensor Networks for Battlefield Surveillance. In: Land Warfare Conference 2006, Brisbane, Australia (October 2006)
7. Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D., Anderson, J.: Wireless Sensor Networks for Habitat Monitoring. In: ACM WSNA 2002, Atlanta, Georgia, USA, pp. 88–97 (September 28, 2002)
8. Wireless Sensor Networks, `http://en.wikipedia.org/wiki/Wireless_Sensor_Networks`
9. Tiny Operating System, `http://en.wikipedia.org/wiki/TinyOS`
10. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceedings of the Symposium Security and Privacy (2003)
11. Du, W., Deng, J., Han, Y., Chen, S., Varshney, P.: A key management scheme for wireless sensor networks using deployment knowledge. In: INFOCOM 2004: Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies (2004)
12. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM Press, New York (2002)
13. Du, W., Han, Y.S., Deng, J., Varshney, P.K.: A Pairwise key predistribution scheme for wireless sensor networks. In: Proceedings of the ACM Conference on Computer and Communications Security (2003)

14. Hoger, K., Andreas, W.: Protocols and Architecture for Wireless Sensor Networks. John Wiley & Sons Ltd., Chichester (2005) ISBN: 0-470-09510-5
15. Raymond, D.R., Marchany, R.C., Brownfield, M.I., Midkiff, S.F.: Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols. IEEE Transactions on Vehicular Technology 58(1), 367–380 (2009)
16. Wood, A.D., Stankovic, J.A.: Denial of Service in Sensor Networks. IEEE Computer 35(10), 48–56 (2002)
17. Wood, A.D., Stankovic, J.A.: Denial of Service in Sensor Networks. IEEE Computers, 54–62 (October 2002)
18. Hu, Y.-C., Perrig, A., Johnson, D.B.: Wormhole detection in wireless ad hoc networks. Department of Computer Science, Rice University, Tech. Rep. TR01-384 (June 2002)
19. Tumrongwittayapak, C., Varakulsiripunth, R.: Detecting Sinkhole Attacks In Wireless Sensor Networks. In: Proceedings of the IEEE ICROS-SICE International Joint Conference, pp. 1966–1971 (2009)
20. Feng, Z., Leonidas, G.: Wireless Sensor Networks (An Information Processing Approach). Morgan Kaufmann Publisher under Elsevier, ISBN: 1-55860-914-8
21. Deepak, G., Alberto, C., Wei, Y., Yan, Y., Jerry, Z., Deborah, E.: Networking Issues in Wireless Sensor Networks. Elsevier Science, Amsterdam (2003), CrossBow Technology Inc., http://www.xbow.com/
22. Hsueh, C.-T., Li, Y.-W., Wen, C.-Y., Ouyan, Y.-C.: Secure Adaptive Topology Control forWireless Ad-Hoc Sensor Networks Journal- Sensors 10, 1251–1278 (2010), http://www.mdpi.com/journal/sensors