Security in Wireless Sensor Networks: Key Intrusion Detection Module in SOOAWSN

Mohammed A. Abuhelaleh and Khaled M. Elleithy
School of Engineering
University Of Bridgeport, Bridgeport, CT
{mabuhela, elleithy} @bridgeport.edu

Keywords: Wireless Sensor Networks, Security, Intrusion Detection System, Clustering Hierarchy.

Abstract

Due to restrictions and limited resources in wireless sensor networks, clustering for routing organization have been proposed literature to increase system throughput, decrease system delay and save energy. Although these algorithms proposed some degree of security, but because of their dynamic nature of communication, most of their security solutions are not suitable. In this paper, we propose two methods of intrusion detection techniques that can be used during wireless sensor networks communications. The proposed solution perfectly fits all kinds of wireless sensor networks that follow the clustering hierarchy distribution. In addition, it may fit many other distribution techniques. The proposed solution is integrated in a complete solution for wireless sensor network that covers all the network lifecycle from the time it deployed which is called Secure Object Oriented Architecture for Wireless Sensor Networks (SOOAWSN).

1. INTRODUCTION

Wireless Sensor Network (WSN) is a special kind of networks. It consists of a number of sensors that sense the surrounding area and forward the collected data to the main node in the network which called a Base Station (BS).

Network monitor is a mandatory requirement in any WSN application to guarantee network stability. The main target for network monitoring is to detect any misbehavior of the network communications. Usually this misbehavior occurs from intruders in the network that may affect the network work or affect the privacy of this network. In this paper, we discuss how to detect such kind of intrusion and how to recover from it.

Our proposed solution fits special kind of WSN distribution which is the clustering hierarchy distribution. In this kind of distribution nodes are grouped into clusters with cluster leaders [1]. These leaders are responsible of forwarding the information from all nodes in the network to the BS. The clustering hierarchy can be categorized into two kinds; static clustering and dynamic clustering. In static clustering, special nodes with special abilities work as leaders during the whole network lifecycle [1]. In dynamic clustering, leaders are regular sensors that change from time to time during the network lifecycle. In both kinds, any attack involves the cluster heads (CHs) will affect all the sensors in its cluster. This results a need to protect these CHs and detect any attacks that may occur [1, 2, and 3].

In this work, we introduce a novel technique to detect any intrusion that may occur during the network lifecycle; especially on the CHs. Prior communication information is to be used to detect any misbehavior in the routing path. In addition, we adopt Public-key authentication. In the first method, a digital signature is used for node-node authentication.

In Section 2, we will discuss some of the related literature on intrusion detection. In Section 3, we present our solution and we discuss criteria that may affect the performance of our solution. In Section 4 we present conclusions.

2. RELATED WORKS

Currently, there are few studies in the area of intrusion detection in WSN. In this section, we present some existing literature on intrusion detection in WSN and Ad-Hoc Networks.

Silva and *et. al.* [4] proposed decentralized intrusion detection in wireless sensor networks. In [4], the authors suggest that nodes to be responsible for monitoring other nodes' behavior. Each node listens to traffic in its radio range to detect any abnormal behavior. These messages are provided to an intrusion detection system. The details of how this system works are not discussed in [4]. This should increase the total power consumption in the network.

Onat *et. al.* [5] propose similar technique to which that has been proposed by Silva and others [4]. The authors do not include details of how the real

intrusion-detection system works. In both [4] and [5], there is no cooperation between monitoring nodes. Instead the detection is executed locally in each node.

Loo *et. al.* [6] proposes Detection for Routing Attacks in Sensor Networks system. The authors assume the similarity of Ad-Hoc Network to WSN. Similarity means that any technique that can applied to Ad-Hoc network can also be applied to WSN. The authors use AODV (Ad hoc On-Demand Distinct Vector) protocol to study the behavior of the network traffic in order to detect any misbehavior.

Bhuse and Gupta [7] present another intrusion detection technique based on DSDV and DSR which are also Ad-Hoc related protocols. They use these protocols to study the network traffic and collect any interesting information that may lead to intrusion detection.

Mishra *et. al.* [8] propose another intrusion detection system that should work smoothly on Ad-Hoc networks applications. In [8], the authors discussed the impact of applying distributed and cooperative intrusion detection architectures on such kind of network.

Marti *et. al.* [9] proposes a mitigating routing misbehavior in mobile ad hoc networks. The authors presented two techniques that can be used as tools for intrusion detection system in Ad-Hoc networks. These techniques are: Watchdog and Path-Rater. In these techniques, recently sent packets are buffered with each overhead packet. In the case of packets matching, the packet in the buffer is erased, since the packet has been forwarded. The main idea is to be sure that all the packets that need to be forwarded are actually sent. In the case the packet stays in the buffer for long time, this should imply that the packet has not been forwarded as it should. A specific threshold is used and compared to the number of times the node detects missing packets to determine the misbehaving of the node.

Saiful *et. al.* [10] propose a Hierarchical Design Based Intrusion Detection System for Wireless Ad Hoc Sensor Network. The authors distribute the responsibility of intrusion detection among three types of nodes. They classified these nodes into layers: Regular-Sensors Layer, Cluster-Heads Layer, and Outer-layer. Each layer is assigned the responsibility of monitoring the lower level layer. CH monitors it group members (i.e. Regular Sensors). Each CH is then monitored by a special node called Regional node. Moreover, each Regional node is controlled and monitored by the BS The main idea of this distribution is to distribute the energy consumption among all network parties. The target of each layer is to study the lower-level layer behavior all the time and notify the upper-level layer with any misbehavior. Even though this technique distribute the power consumption on the whole network, it is still consumes the same power as other proposals.

3. NEW INTRUSION DETECTION MODEL

This model contains two methods for detecting intruders in the network. Both methods can be used together or independently.

The first method uses Public and the Private keys to authenticate the sensor. When sensors receive messages from other sensors they use the public and private key technique to ensure the authenticity of the other sensors. Anytime a sensor suspects the behavior of any other sensor, it will report it in the message that is going to the BS Then, the BS compares the suspected sensor ID with the IDs in a table contains all sensors IDs. If the ID does not exist in its table, the BS broadcasts a warning signal to all sensors to ignore future communication with that sensor. If the ID exists, then there is a probability that this sensor has been compromised. In this case, the BS stores the sensor information in a table called Suspected-Nodes table. If the BS receives more than one warning, then it will react. It will send a small message to the suspected sensor encrypted using the secret key.

The message will also include a nonce (a special value changes in a specific way decided by the BS prior to network deployment) that is encrypted using the same suspected sensor public key. The nonce has to be increased by a specific unique value stored earlier in each sensor. Then, the sensor sends back the signal with the modification, using the secret key. The BS then checks the updated value after decrypting the message, and compares it with the expected value. If it does not match, then it considers this sensor a compromised sensor and it informs all other sensors with the compromised one. Any transaction from that compromised sensor will be ignored and any sharing key with that sensor will be terminated or renewed.

In the second method we consider when any sensor sends a report to the BS It includes the previous activities for itself (i.e. the previous CH ID and the sequence number of the message). These activities contain the ID of the CH who was responsible for forwarding the previous message from that sensor. The serial number of the message is also included in the activity part of the report. BS stores all activities in the network. Each time the BS receives new information, it compares it with the information it has regarding the activities. Any missing or mismatching information will conclude that there is a problem that may involve two parties, the sensor itself and its previous CH. To be sure that the BS reacts efficiently to this problem, it doesn't react until the mismatching relates to the same CH or

the same sensor is repeated more than once. Accordingly, it will decide if the node is compromised or there is an intruder.

Recovery from intrusion detection depends on the reaction of the BS to such detection. The most important part is to isolate this intruder or the compromised node from the whole network. The second part is to deactivate all keys that could be known by the intruder.

3.1 Digital Signature Method

In this Method, Public and the Private keys are used to authenticate the sensor. The algorithm works as follows (Figure1):

1) Sensor A send a message to sensor B. Part of this message (i.e. signature) is encrypted using A's private key. The signature part consists of A's ID and a nonce.
2) Sensor B decrypt the signature part using A's public key. It then compares this part with the external part that consists of A's ID and the nonce. If they are not matched, then A's is considered as a suspected node.
3) If sensor B detects any suspected node, it informs the BS of that node. In order not to consume extra energy, sensor B sends this information as part of its regular report.
4) The BS compares the suspected sensor ID with the IDs in a table contains all sensors IDs.
    a. If the ID does not exist in its table then go to step6.
    b. If the ID exists then the BS stores the sensor information in a table called Suspected-Nodes table.
5) If suspected sensor ID's is found in the suspected table then go to step6.
6) The BS broadcasts a warning signal to all sensors to ignore future communication with that sensor and terminate or renew all the keys that are shared with that sensor

This method provides powerful detection mechanism to detect any intruder trying to attack the network.

This method results in few data overhead that is produced from the addition part added to the original message, which is the digital signature. However, we try to reduce the attributes needed to build this signature using only the sensor ID and the nonce. This will decrease the data overhead required to build such signature compared to traditional Public key authentication that is used in the traditional networks.

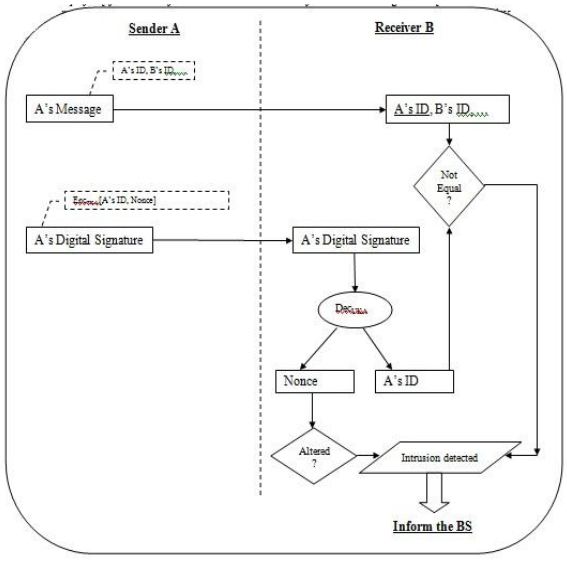
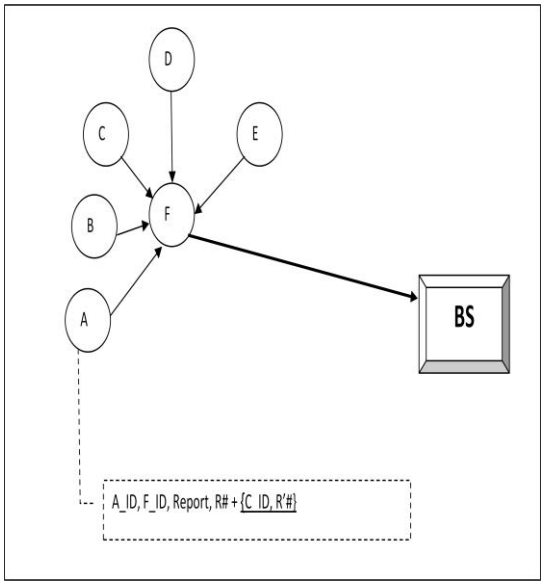


Figure1. Using Digital Signature for node authentication

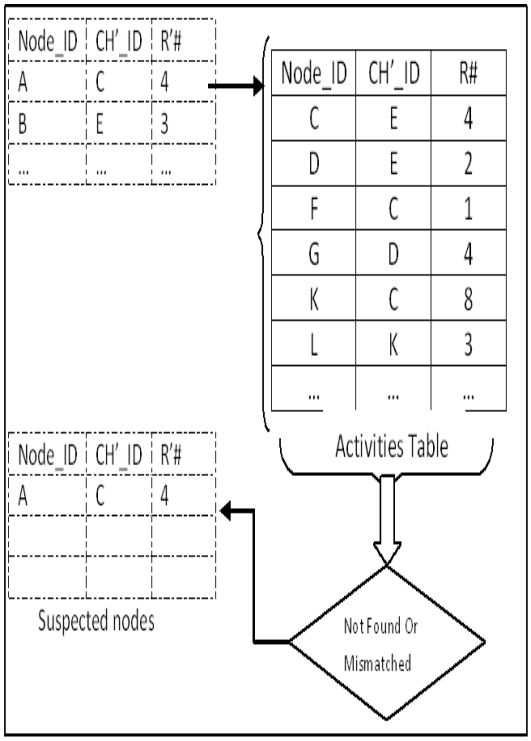
3.2 Routing Attack Method

This method provides an ability to detect any attack that may affect the information forwarded to the BS. The algorithm works as follows:

1) Sensor A includes its previous activity in the report forwarded to the BS This activity contains the ID of the CH who was responsible of forwarding the previous message from that sensor. The serial number of the message is also included in the activity part of the report (Figure2. a.).
2) The BS stores all activities (i.e. nodes IDs with their related CHs and sequence numbers of the messages) in the network, and each time it receives new information, it compares it with the information it has regarding the activities. Any missing or mismatching information will indicate a problem that may involve two parties, the sensor itself and its previous CH (Figure2. b.). The activities table size should be determined depends on the network size and nature of the application. When the data stored in the table reach the size, then the new data will overwrite the old data.
3) If the BS finds a frequent information mismatching related to the same CH or the same sensor, it will decide the compromised node or the intruder.
4) The BS broadcasts a warning signal to all sensors to ignore future communication with that sensor and terminate or renew all the keys that are shared with that sensor.



a) BS analyzes the messages received from the sensors via their CHS



b) BS checks the accuracy of the received information

Figure2. Filling Suspected node table in Routing Attack Method

In this method, the number of sensors compares to the number of CHs in the network will determine the efficiency of its function.

Increasing the number of sensors for a constant number of CHs will result that each CH has higher number of sensors in its group. In case that this CH has been compromised or in case that it is an intruder, then the number of reports that are going to be sent to the BS in the next round will be higher. This will help the BS to make a quick decision regarding this attack. On the other hand, this will lead to more damage to the network in that specific cycle where the attack occurs. This concluded from the high number of the sensors connected with that CH. It is the responsibility of the BS to choose a typical percentage of desired CHs which is to be changed during the network lifecycle depends on the number of sensors in the network.

Figure 3 shows the relation between the number of reports sent to the BS and the number of CH in an N size network. It shows different values ranging from 100 sensors network size to a 1000 sensors network size with different percentages of the desired CHs ranging from 0.01 to 0.1. It shows that from a specific network size, the increase of the desired percentage of CHs will decrease the number of the nodes involved in the attack which will also decrease the number of the reports that sent to the BS in the next round.

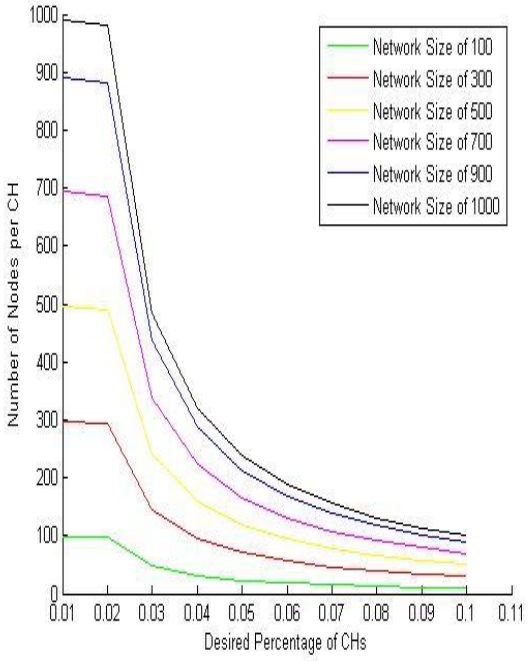


Figure3. Number of reports send to the BS depends on the number of sensors compared to the number of CHs.

Figure4 shows the same relation with more details for different network sizes with different percentages of CHs. It shows the average number of reports sent to the base station under different values of network sizes and desired percentage of CHs.

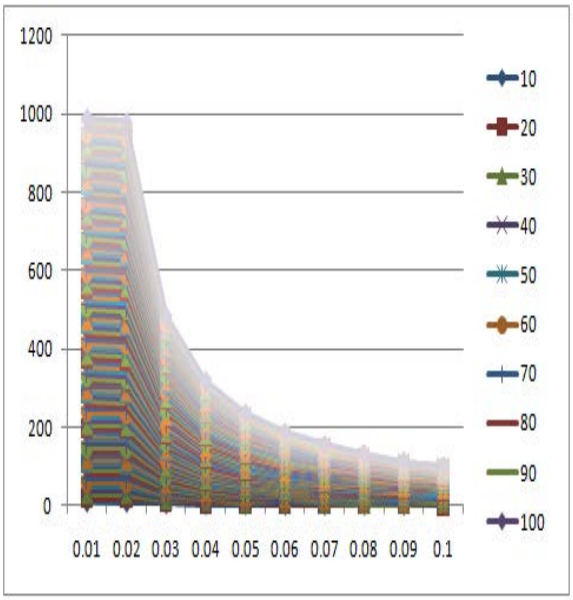


Figure4. Average number of reports sent to the BS under different network sizes with different percentages of CHs

4. CONCLUSION

In this paper we propose a new model for intrusion detection in WSN. The method contains of two methods that cover the detection of unauthenticated nodes and the detection of routing attack. This model is integrated in SOOAWSN framework. The simulation shows how performance parameters are affected by the network size and the desired percentage of CHs in such network. This flexibility allows our proposed protocols to be adopted in different applications for WSN.

References

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan., "Energy-efficient communication protocol for wireless microsensor networks", in IEEE Hawaii Int. Conf. on System Sciences, pages 4–7, january 2000.

[2] S. Selvakennedy, and S. Sinnappan., "A Configurable Time-Controlled Clustering Algorithm for Wireless Networks", 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.

[3] Manjeshwar and D. Agrawal., "Teen: A routing protocol for enhanced efficiency in wireless sensor networks", in 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, 2001.

[4] P. Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile network (Q2SWinet '05). ACM Press, October 2005, pp. 16–23.

[5] Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, Montreal, Canada, August 2005, pp. 253–259.

[6] E. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," International Journal of Distributed Sensor Networks, 2005.

[7] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006.

[8] Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," IEEE Wireless Communications, vol. 11, no. 1, pp. 48–60, February 2004.

[9] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000) August 6-11, 2000, Boston, USA. Boston, MA, ACM Press, pages 255-265.

[10] M. Saiful, I. Mamun and S. Kabir, "HIERARCHICAL DESIGN BASED INTRUSION DETECTION SYSTEM FOR WIRELESS AD HOC SENSOR NETWORK", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.

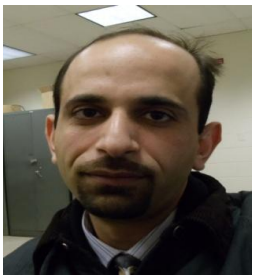
Biography

Dr. Elleithy is the Associate Dean for Graduate Studies in the School of Engineering at the University of Bridgeport. He has research interests are in the areas of network security, mobile communications, and formal approaches for design and verification. He has published more than one hundred twenty research papers in international journals and conferences in his areas of expertise.

Dr. Elleithy is the co-chair of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). CISSE is the first Engineering/Computing and Systems Research E-Conference in the world to be completely conducted online in real-time via the internet and was successfully running for four years.

Dr. Elleithy is the editor or co-editor of 10 books published by Springer for advances on Innovations and Advanced Techniques in Systems, Computing Sciences and Software.

Dr. Elleithy received the B.Sc. degree in computer science and automatic control from Alexandria University in 1983, the MS Degree in computer networks from the same university in 1986, and the MS and Ph.D. degrees in computer science from The Center for Advanced Computer Studies in the University of Louisiana at Lafayette in 1988 and 1990, respectively.



Mohammed Abuhelaleh is a full-time Ph.D. student of Computer Science and Engineering at the University of Bridgeport. He worked as a lecturer for Alhusein Bin Talal University/Jordan; He taught some computer science courses, in addition to college courses, like Data Structure, C++, and Computer Skills for three years.

Mohammed has master degree in Computer Science from University of Bridgeport/ CT, USA, and graduated with a GPA of 3.48. Mohammed worked as Graduate Assistant for many times under Prof. Elleithy. Mohammed now is at the end of the Ph.D. program. He is currently working as an administration assistant and a teaching assistant with Prof. Elleithy.