# SECURITY IN WIRELESS SENSOR NETWORKS – IMPROVING THE LEAP PROTOCOL

Delan Alsoufi[1], Khaled Elleithy[1], Tariq Abuzaghleh[2] and Ahmad Nassar[1]

[1]Department of Computer Engineering, University of Bridgeport, CT, 06604
dalsoufi@bridgeport.edu, elleithy@bridgeport.edu,
anassar@bridgeport.edu
[2]Department of Electrical Engineering, University of Bridgeport, CT, 06604
tabuzagh@bridgeport.edu

## ABSTRACT

*Wireless sensor networks are becoming significantly vital to many applications, and they were initially used by the military for surveillance purposes. One of the biggest concerns of WSNs is that they are very defenceless to security threats. Due to the fact that these networks are susceptible to hackers; it is possible for one to enter and render a network. For example, such networks may be hacked into in the military, using the system to attack friendly forces.*

*Leap protocol offers many security benefits to WSNs. However, with much research it became apparent that LEAP only employs one base station and always assumes that it is trustworthy. It does not consist of defence against hacked or compromised base stations. In this paper, intensive research was undertaken on LEAP protocols, finding out its security drawbacks and limitations. A solution has been proposed in order to overcome the security issues faced in implementing this protocol whilst employing more than one base station. The performance of the proposed solution has been evaluated and simulated to provide a better network performance.*

## KEYWORDS

*Network Protocols, Wireless Sensor Network (WSN), LEAP protocol, Security, compromised nodes*

## 1. INTRODUCTION

Wireless technology has propagated the use of sensor networks in many applications. Sensor networks join small sized sensors and actuators with general purpose computing components [1]. Such networks comprise of hundreds and sometimes thousands of self-functioning, low power, inexpensive wireless nodes to observe and influence the surroundings.

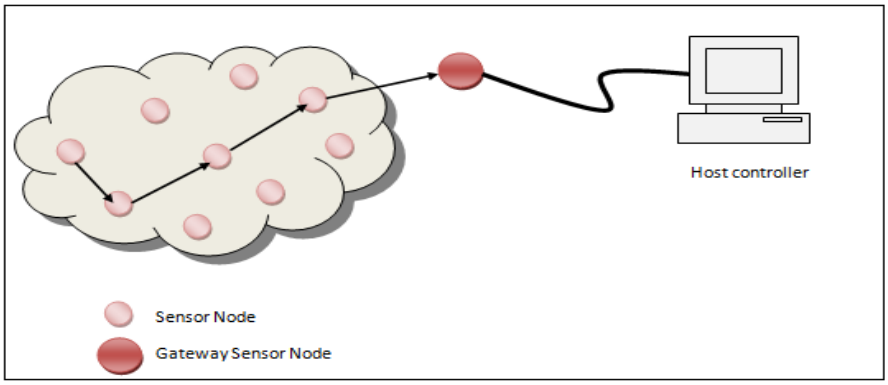



Figure 1. Example of a Wireless Sensor Network

DOI : 10.5121/ijcses.2012.3301 

Wireless sensor networks usually consist of a single or multiple base stations acting as points of centralized control, whereby they provide access to other networks. These networks are unique in their dynamic network topologies. A network topology is usually selected depending on the type of application the sensors are used for or where it is situated. The types of topologies used for sensor networks include star, mesh, star-mesh etc. [2]

In Wireless sensor networks there are two kinds of wireless nodes; sensor and base station nodes. The main function of the base station (also referred to as sinks) relies on managing the actions executed to provide reliable and efficient sensing support. It provides a gateway to other networks or acts as a data storage processing data in a powerful way [3]. It even acts as an access point to human interface for human interaction, and is capable of broadcasting control data in the network or removes data from it. The base station node will calculate and send the even source, its position and a timestamp to the analysis centre. If an alert is received by the base station regarding a target, an identity of the target will be allocated allowing all related alerts getting appropriate management.

Every sensor within the network primarily consists of a certain amount of power and a base station that provides entrance to other networks or to the centre analysis. It is important to know that base stations have significant features over other nodes in the network. They comprise of adequate battery power to exceed the existence time of all sensor nodes, and have the capacity to save cryptographic keys, well-built processors and resources to commune with external networks.

In contrast to the base stations, in a sensor network a large number of sensor nodes are connected together with radio frequency communication links, giving much significance to broadcasting in the network [1]. Protocol procedure plays a vital role. Although they have concerns with trust assumptions, energy usage is decreased when using these protocols. The main purpose of these nodes is to gather information or events occurring from their targets. The main functions associated with sensor nodes include: collecting information on the target with consideration to their nature and positioning, which involves the communication from nodes to base stations regarding for example sensor readings and particular alerts.

Nodes should be capable of producing real-time events on detected targets using the base station node to forward an even transmission to a centre for the event to be analyzed [4]. Base stations may request updates from sensor nodes, resulting in base station to node communication.

Finally the generated events will be relayed to the base station from the sensor nodes. In this part of the communication architecture, base stations contact all of the nodes it is assigned for purposes such as routing beacons or reprogramming of the complete network.

Given that sensor networks usually compose of nodes that are not physically protected in certain environments, these networks contain further vulnerabilities to security threats. Some of these security threats include passive information gathering, Sink-hole attacks, Wormhole attacks, false node and malicious data and so forth.

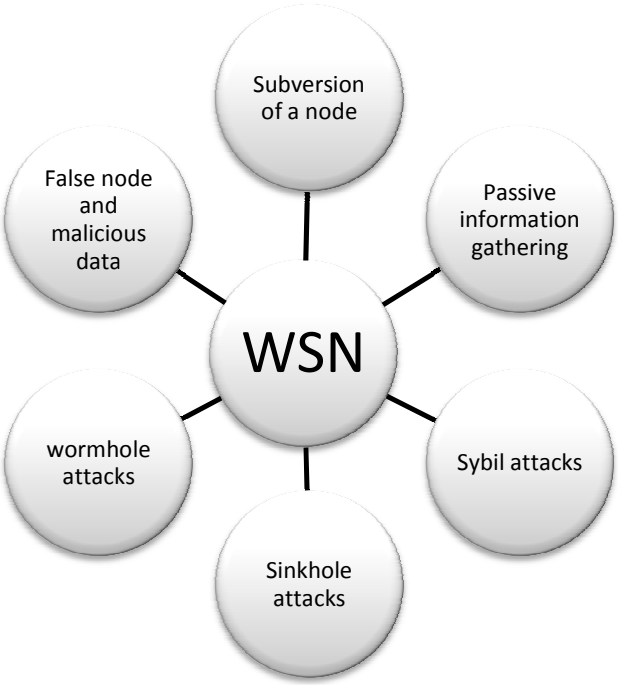



Figure 2. WSNs and common attacks

In the attempt to conquer all of these factors which affect the designs of Wireless sensor networks, we have to trade off performance or expenses so that these liabilities are decreased to tolerable levels. Due to the fact that such factors are motivated by cost and application level performance and energy, to minimize their affects, it is preferable sometimes to acquire sensor hardware that is more efficient in terms of security and consist of more than one base station. This, of course, is more expensive than sensors having a single base station. When working with protocols, software or certain services, sometimes there is a need for trading of performance or cost for security.

This paper proposes a solution to some of the security issues faced in WSNs. In particular, the paper focuses on LEAP protocol taking into consideration its advantages and attempts to overcome its disadvantages.

## 2. LEAP PROTOCOL

LEAP is also a very popular security solution in Wireless Sensor Networks and it was proposed by Zhu et al in 2004. The Localized Encryption and Authentication Protocol (LEAP) is a key management protocol used to provide security and support to sensor networks. It uses μTESLA to provide Base station broadcast authentication and a one-way-hash-key to authenticate source packets [5]. This protocol is inspired by the idea that every message broadcasted between sensor-nodes is different from another and comprise of different security requirements. In order to meet the variety of security requirements when exchanging messages, having a single key mechanism is impractical, thus LEAP proposes four types of keys assigned to every individual node. The four types of keys established are: individual keys, pair-wise keys, cluster keys and group keys [6].

## 2.1 Individual Key

The Individual key is a unique key shared between a node and its corresponding base station in order to provide security between them as they commune. Communication between a node and a base station is vital as it allows a node to inform the base station of any abnormal behavior detected from its surrounding nodes. As a result, the base station being aware of the malicious node can then use the key to encrypt the important information such as instructions to a specific node. The individual key can be fabricated using the following equation:

$$k_u = \rho k_i(ID_u)$$

Where $\rho$ is the pseudo random function, $k_i$ is the initial key, also known as the master key and $ID_u$ is the ID of node u

## 2.2 Pair-wise Key

The pair-wise key is a key shared between a node and its neighbouring sensor nodes. The establishment of this key ensures protection of communication that longs for privacy or authentication of a source. The advantage of having a pair-wise key secures transmission because it is shared between a node and one of its immediate neighbors and therefore prevents it from intruders. After the individual key has been set up, nodes can then identify their neighbors by sending out a message with its ID waiting for a response from the neighbor node n. The Pair-wise (Kp) key can be fabricated by the following equation:

$$k_n = \rho k_i(ID_n)$$

u $\rightarrow$ * : $ID_n$, $Nonce_u$

$n \rightarrow u : ID_n, MACK_n(Nonce_u|ID_n)$

Thus,

$$k_p = \rho k_n(ID_u)$$

## 2.3 Group Key

A group key, also known as the global key is shared by all the sensor nodes within the network. The base station uses this key to encrypt data that is transmitted to all the nodes within the group. Since the entire group of nodes is sharing this key, it eliminates the need for a base station to separately encrypt the same message to individual nodes with individual keys. Confidentiality is invoked as long as the key is updated every once a while in case one of the nodes stops functioning and is removed from the group or network. A special case of a group key is known as the cluster key.

## 2.4 Cluster Key

The cluster key is a key shared by a node with multiple of its neighboring sensor nodes. The cluster key is generated by node u using a random function and encrypts this key using the pair-wise key so that only the authenticated neighbors are able to decrypt to get access to the cluster key. Hence, Kc (cluster key) is generated randomly by node

$$u \rightarrow n_i : (k_c)\, k_{pi}$$

The advantages of this protocol are simply that it reduces the participation of a base station and it is efficient in terms of communication and energy. Its security purposes mainly cover local communication such as routing information and protecting messages sent from the nodes. The establishment of this key allows nodes to decrypt and authenticate certain messages like readings from neighboring nodes. Therefore, LEAP permits the use of cluster keys which one node may use to protect its data allowing only authenticated neighboring nodes to obtain and decrypt this data.

All in all, it can be stated that LEAP protocols are very advantageous in that they offer mechanisms for authenticating both: broadcasting of a base station and source packets, as well as mechanisms providing key revocation and refreshing. Other advantages LEAP presents a network are its scalability and cluster communication abilities.

However, the major disadvantage of this protocol, which can influence the network most, is that it only consists of a single base station and assumes that it is never compromised [7]. Other drawbacks include security weakness that is present during the process of key establishment, and the high cost of capacity needed to store the four different keys for each node, when the number of nodes is small.

In the leap protocol, several efforts are made through the use of the keying mechanisms to ensure that a compromised node is revoked or at least prevent it from slowing the network operations. On the other hand, the LEAP protocol lacks in preventing attacks on the base station itself, which happens to be very critical as the base station covers a large network operational area.

## 3. PROPOSED SOLUTION: IMPROVED LEAP PROTOCOL

In literature, the majority of the key management protocols usually focus on the aspect that only a singular base station or sink node is used in a WSN and these protocols assume that it is trustworthy. For some systems, however, several sink nodes are used [8]. In these systems, two important things must be considered: cost and security.

In the leap protocol, several efforts are made through the use of the keying mechanisms to ensure that a compromised node is revoked or at least prevent it from slowing the network operations. A base station, on the other hand, will be treated the same as any compromised node and the idea is to apply the same mechanisms used to overcome a compromised node to also prevent a hacked base station node.

With a lot of excessive research, the literature usually covers WSN functionalities in terms of one base station participating in one system. It is important to remember that with an increase in a sensor network there's an increase in the distance separating the base station and its related sensor nodes and the increase in the distance may alter the following:

- With a long distance for packets to propagate through, they may get lost on the way resulting in network performance degradation.

- Data transmissions between sensor nodes and a single base station in a large network require high energy consumptions giving the need to reduce the lifetime of nodes.

- For the nodes that are situated nearby a base station, their energy is worn out rapidly, which in turn shortens the network life time very drastically.

To overcome these problems, a network employing several base stations shows potential in bettering the performance. However, there is of course the tradeoff between performance and cost. By deploying more than one sink node in a network may be costly, but the distance between the sink nodes and its associated sensor nodes will be reduced providing more successful paths for data transmission as well as eliminating the disadvantage of the high energy consumptions otherwise faced.

For this research, a WSN with several base stations will be considered. Under the circumstances that a base station and a sensor node are compromised, an evaluation of the network performance will be analyzed.

Wireless sensor networks provide the advantage of using a large number of nodes (from a hundred up to thousands of nodes) communicating with each other inexpensively. One or more base stations process all of the network functions. Should there be a need to increase the number of sink nodes, one has to consider enhancement in expenses. The LEAP protocol offers much security to a system with the establishment of the four keys, mentioned previously. The protocol consists of key revocation and refreshing mechanisms in the attempts to successfully avoid or deal with compromised sensor nodes.

The methods used in detecting the isolated compromised nodes are done through μTESLA and one-way key chain hash authentication functions [9]. However, this protocol lacks in security against a base station, should it be compromised, and network robustness. These are significant aspects to consider because if a sink node is compromised, it could severely affect the entire network or system as all the network functions are dealt by these nodes. The flexibility feature of a LEAP protocol is advantageous over many other security protocols used, but improvements in robustness are needed. Therefore, to improve the LEAP protocol, a solution is proposed to overcome the limitations faced for possible attacks on the base stations itself and thereby adding more robustness to the network system in terms of recovering from a compromised base station as well as a compromised sensor node.

In theory, the majority of research papers, consider the presumption of a reliable base station and only take measures for compromised nodes. In isolated locations, it is relevant to be vigilant in case a base station is compromised. Security against higher levels of attacks against a base station, which usually occur from sources with higher computational power, is a necessity [10]. In a wireless sensor network, three courses of actions can occur:

- A sensor node is compromised
- A base station is compromised
- Sensor nodes and base stations are compromised concurrently

The LEAP protocol only consists of actions that deal with the first scenario. In improving the LEAP protocol, all three scenarios have to be dealt with, thus a network has to be built with more than one base station. So, by ensuring that the LEAP protocol is able to handle all three scenarios aforementioned, the LEAP protocol will be improved in terms of security for WSNs.

I used the same mechanisms as the original LEAP protocol to overcome compromised sensor nodes, and added another similar mechanism to detect if any of the base stations are to be compromised. For this solution, I had to establish another key, called the Base station key (Kb). The base station key will also be updated periodically, and it is shared amongst the base stations. If a base station is hacked, it will not be aware of the updated session key, and continue

to use its old key. In doing so, the base station will not be involved in the data transmission, and the other remaining base stations will identify that this base station is compromised.

The authenticated base stations will send the administrator a message indicating that one of the base stations is hacked. It is then up to the administrator to remove it from the system or replace it with another one. However, there is always a case whereby the opponent base station will act like an authenticated node and accuse one of the other validated base stations of being hacked. The administrator will consider any of the base stations to be hacked if at least more than one of the remaining three base stations declares otherwise.

## 4. RESULTS AND CONCLUSIONS

To evaluate the proposed solution, an algorithm has been developed to simulate a sensor network using the MATLAB program. The whole idea was to implement a system whereby multiple base stations have been employed for the soul purposes of improving the data transmissions amongst nodes and to come up with a solution for a base station, should it be compromised.

The LEAP protocol was implemented and simulated using one base station and fifty sensor nodes situated randomly. Initially, an individual key was generated for each node from a randomly generated master key. Then a cluster key was generated by each node and published to their neighboring nodes using the pair-wise keys. Finally, the global key was generated in order to enable public broadcasts.

Figure 3 shows an ideal case for the LEAP protocol. It simply represents a base station surrounded by fifty sensor nodes. In this scenario, none of the nodes are compromised. However, even though it is an ideal case, we still face the problem of data loss. For arguments sake, let's assume that node z wants to communicate with the base station. Having a singular base station means that no matter how far the distance, the sensor node and the base station will commune with each other. The longer the distance, however, the more nodes they have to transmit through, the more bandwidth will be used and the higher the possibility of loss of data.

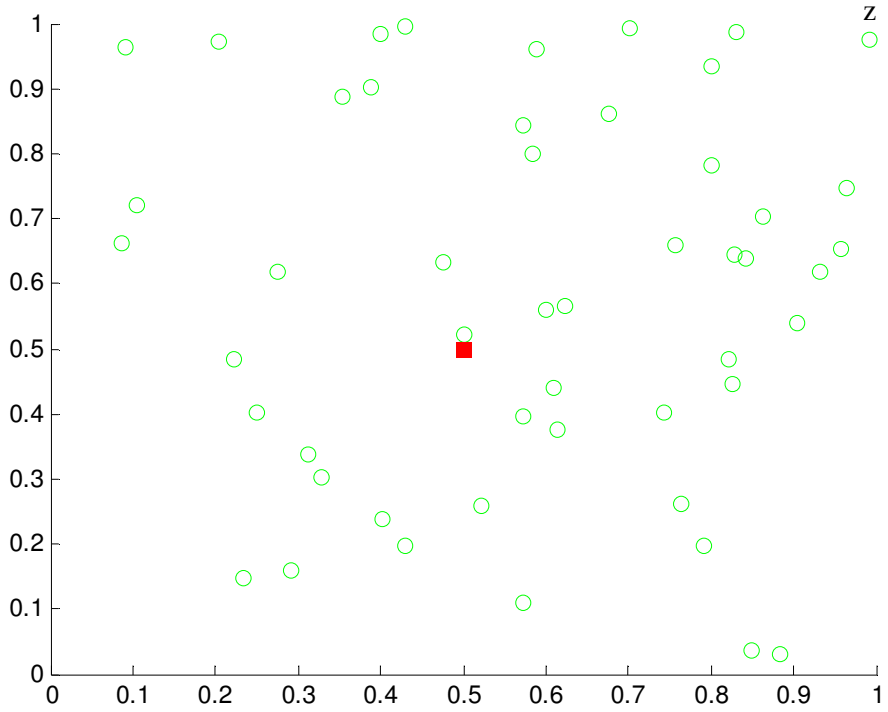



Figure 3. LEAP protocol: Ideal scenario

Figure 4 shows the scenario of a compromised node. The node that is labelled symbolizes a node that has been hacked. As mentioned throughout this paper, the LEAP protocol is very efficient when it comes to dealing with compromised nodes. With its key refreshing and revocation schemes, if a node is affected, these mechanisms prove advantageous. With the many keys assigned to all the sensor nodes with its periodic updates, if one of the nodes is unable to decrypt an updated key, the compromised node will not be able to further participate in the data transmission which will then inform the surrounding nodes and eventually the base station that this node is no longer wanted. The compromised node will be removed.

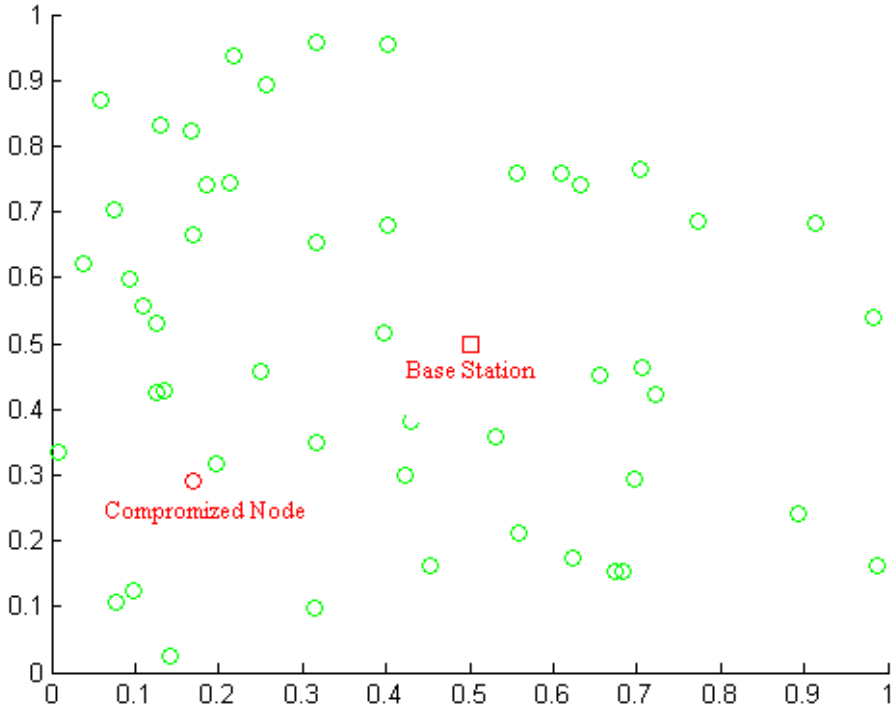



Figure 4. LEAP protocol: A compromised Sensor Node

In order to simulate and test the performance of the proposed improved LEAP protocol, a WSN of hundred sensor nodes situated randomly, and four base stations also situated randomly has been generated.

Figure 5 shows the improved LEAP protocol in an ideal scenario, whereby multiple base stations are supported. Depending on the distance between the nodes and the base stations, each sensor node was assigned to its closest base station. The four different colors (red, blue, green and black) are used in order to distinguish between the base stations and its corresponding sensor nodes.

This diagram illustrates an ideal scenario whereby none of the nodes or the base stations are compromised. The use of four base stations provides an advantage over the existing LEAP protocol. The idea that more than one base station has been used, the nodes will not need to transmit to a base station that is extremely distant from it, which means that it minimizes the problem most networks sometimes face regarding lost data during transmission.

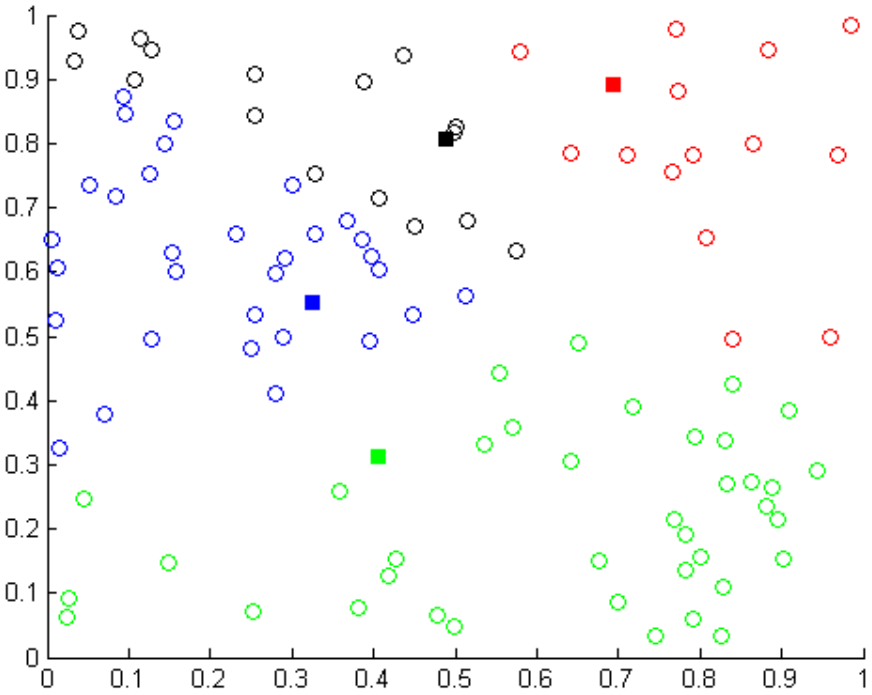



Figure 5. Improved LEAP protocol: Ideal Scenario

Figure 6 demonstrates the scenario whereby a base station is compromised. A hacked base station can be detected and revoked by the other base stations using the new generated key known as base station key (Kb). If a base station is hacked, it will not be aware of the updated session key, which is also updated periodically, and continue to use its old key. In doing so, the base station will not be involved in the data transmission, and the other remaining base stations will identify that this base station is compromised. The authenticated base stations will send the administrator a message indicating that one of the base stations is hacked. It is then up to the administrator to remove it from the system or replace it with another one. However, there is always a case whereby the opponent base station will act like an authenticated node and accuse one of the other validated base stations of being hacked. The administrator will consider any of the base stations to be hacked if at least more than one of the remaining three base stations declares otherwise.

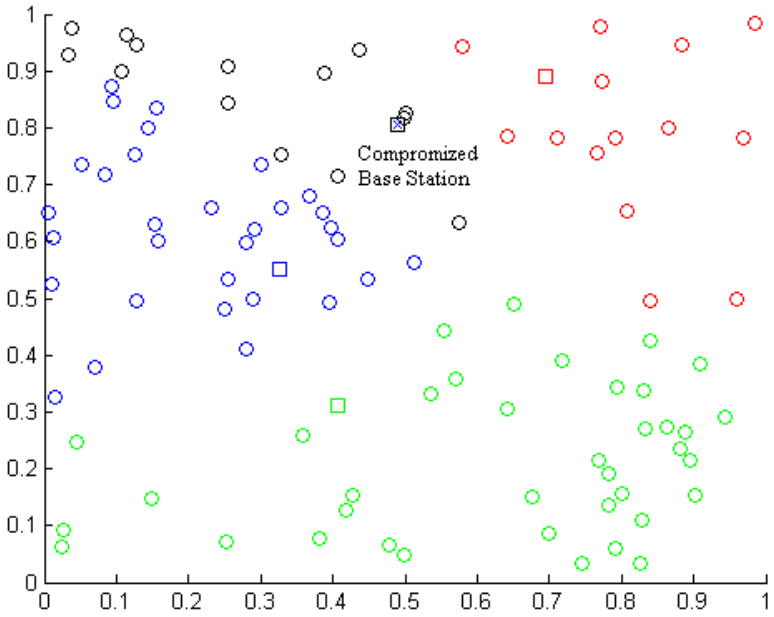



Figure 6. Improved LEAP protocol: A compromised base station

In this solution, the LEAP protocol was improved in terms of using multiple base stations for the purpose of minimizing loss of data transmissions, and also the proposed solution was able to detect a compromised base station. In using multiple base stations, the performance of the system is improved but the cost of implementation is increased. Table 1 shows a comparison between the LEAP and the improved LEAP protocols.

Table 1. Comparison between LEAP and Improved LEAP protocols

| | **LEAP** | **Improved LEAP** |
|---|---|---|
| **Detects and removes Compromised Sensor Nodes** | Yes | Yes |
| **Detects and removes compromised base stations** | No | Yes |
| **Data Loss** | High | Minimal |
| **Cost** | Low | High |
| **Bandwidth use** | High | Low |
| **Transmission Delay time** | High | Low |
| **Energy consumption** | High | Low |
| **Node lifetime** | Low | High |

## REFERENCES


[1] Saraogi, M. (n.d.). Security in wireless sensor networks. University of Tennessee,

[2] Burgner, D. E., & Wahsheh, L. A. (2011). Security of wireless sensor networks. Eighth International Conference on Information Technology: New Generations,

[3] Madden, S. R., Franklin, M. J., Hellerstein, J. M., and Hong, W., TAG: A tiny aggregation service for ad-hoc sensor networks. In The Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), 2002,

[4] Madden, S. R., Szewczyk, R., Franklin, M. J., and Culler, D. Supporting aggregate queries over ad-hoc wireless sensor networks. In Workshop on Mobile Computing and Systems Applications, 2002,

[5] Zhu, S., Setia, S., Jajodia S., LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In The Proceedings of the 10th ACM conference on Computer and communications security, 2003.

[6] Jang, J., Kwon, T., & Jooseok, S. (2007). A time-based key management protocol for wireless sensor networks. E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 314–328, 2007.,

[7] Pathan, A. K. (2011). Security of self-organizing networks. (1 ed., pp. 318-344). Florida: CRC Press.

[8] Saraogi, M. (n.d.). Security in wireless sensor networks. University of Tennessee,

[9] Jang, J., Kwon, T., & Jooseok, S. (2007). A time-based key management protocol for wireless sensor networks. E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 314–328, 2007.,

[10] Zhu, S., Setia, S., Jajodia S., LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In The Proceedings of the 10th ACM conference on Computer and communications security, 2003.

[11] Modares, H., Salleh, R., & Moravejosharieh, A. (2011). Overview of security issues in wireless sensor networks. Third International Conference on Computational Intelligence, Modelling & Simulation, IEEE,

[12] Abuhelaleh, M. A., & Elleithy, K. M. (2010). Security in wireless sensor networks: Key management module in sooawsn. International Journal of Network Security & Its Applications (IJNSA), 2(No. 4),

[13] Mohanty, P., Panigrahi, S., Sarma, N., & Satapathy, S. S. (2010). Security issues in wireless sensor network data gathering protocols: A survey. Journal of Theoretical and Applied Information Technology,

[14] Perrig, A., Szewczyk, R., Wen, V., Culler, D., & Tygar, J. D. (2001). Spins: Security protocols for sensor networks. Mobile Computing and Networking 2001,

[15] Wang, Y., Ramamurthy, B., & Xue, Y. (2008). A key management protocol for wireless sensor networks with multiple base stations. CSE Conference and Workshop Papers. Paper 111.,

[16] Wang, Y., Ramamurthy, B., & Xue, Y. (2008, January 1).Digitalcommons@university of nebraska - lincoln. Retrieved from http://digitalcommons.unl.edu/cseconfwork/111

[17] Xue, Y., Lee, H. S., Yang, M., & Kumarawadu,, P. (2007). Performance evaluation of ns-2 simulator for wireless sensor networks. 0840-7789/07 ©2007 IEEE,

[18] Söderlund, R. (2006). Energy efficient authentication in wireless sensor networks. LITH-IDA/DS-EX--06/012--SE,

[19] Perillo, M. A., & Heinzelman, W. B. (n.d.). Wireless sensor network protocols. Department of Electrical and Computer Engineering University of Rochester,

[20] Tun , Z., & Maw, A. H. (2008). Wormhole attack detection in wireless sensor networks. World Academy of Science, Engineering and Technology 46 2008,

[21] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister. System architecture directions for networked sensors. In Proceedings of ACM ASPLOS IX, November 2000,

[22] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song. Efficient authentication and signing of multicast streams over lossy channels. In IEEE Symposium on Security and Privacy, May 2000.

[23] Karlof, C., Sastry, N., Wagner, D. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. ACM SenSys 2004, November 3-5, 2004.

[24] Y.C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[25] P. Apostolos, "Cryptography and Security in Wireless Sensor Networks," FRONTS 2nd Winterschool Braunschweig, Germany, 2009.

[26] Chris Karlof David Wagner. In Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.

[27] Y. Hu, A. Perring, and D.B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In Proceedings of 22nd Annual Conference of the IEEE Computer and Commu-nication Societies, Vol.3, April 2003. pp.1976-1986.

[28] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. CCS'02. New York, NY, USA: ACM Press, 2002, pp. 41–47.

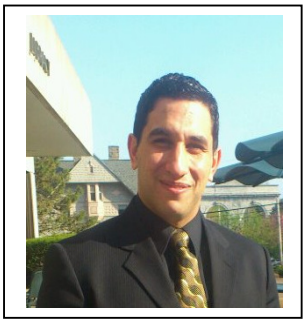
[29] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6),

**Authors**

**Delan Alsoufi** received her Master degree in Computer Engineering at the University of Bridgeport, in 2012 with a GPA of 3.82. Her research area is on Wireless sensor network security. After the completion of her Master degree she's going to Iraq to work as an Instructor in the computer engineering department at the University of Duhok, Kurdistan.
She grew up in London, UK, where she completed the 13compulsary years of education. In 2005 she moved to Iraq and completed her B.Sc. degree in Electrical and Computer Engineering from University of Duhok. In 2010 she received the prestigious Fulbright scholarship to pursue her graduate studies in the United States.

**Khaled 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 fifty research papers in international journals and conferences in his areas of expertise. He 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. He 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. He 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.

**Tariq Abuzaghleh** completed his Masters in Electrical Engineering in 2012 from the University of Bridgeport, Connecticut, and graduated with a GPA of 4.00. His research areas are image processing techniques and network security. He has published several research papers in these areas in well recognised journals and conferences. He has been working as a research assistant in university of Bridgeport in the last two years. He grew up in Amman, Jordon, and after receiving his B.Sc. degree in electrical engineering; he worked as a broadcasting engineer for two years and is currently attempting to pursue his educational knowledge by undertaking a Ph.D program.



**Ahmad Nassar** completed both his B.Sc. and M.Sc. in computer engineering at the University of Bridgeport. For his Masters degree, he received a GPA of 3.82. During his graduate studies, he worked as graduate assistant in the lab operations in the engineering school where he broadened his knowledge in the field of computer networking and security. Currently he is working in Virtusa, Connecticut, as a software developer.