International Journal of Computer and Electrical Engineering, Vol. 1, No. 3, August 2009
1793-8163

Desirable Security for Wireless Sensor Networks

Akbar Abbasi, *Member, IACSIT*

***Abstract*— Sensor networks will play a key role in future smart environments. Sensor nodes which are used to form wireless sensor networks, are limited energy resources and have low power capabilities. Thus, sensor networks need to be energy efficient. When they are deployed in military environments, they also need strong security services.**

In this paper, an energy-efficient security protocol is proposed for resource constrained sensor networks. The proposed protocol provides a security mechanism to detect energy consuming and useless packets that enemy injects into sensor network. Both mathematical analysis and simulation of this protocol are provided in this paper.

***Index Terms*—- Sensor network, Security, Energy consumption**

I. INTRODUCTION

Advances in wireless communication and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes [1]. These tiny sensor nodes consist of sensing, data processing, and communicating components [2]. The sensor nodes can sense physical information, process crude information, and send them to the sink. Security concerns constitute a potential stumbling block to the impending wide deployment of sensor networks [3]. Nowadays, designing a scalable secure sensor network that has low energy consumption is a challenging issue. In this paper, an energy-efficient security protocol is proposed which provides a strong security and decreases energy consumption.

II. HIERARCHICAL STRUCTURE

A flat structure with a powerful base station and sensor nodes is clearly not scalable to a large number of nodes. Thus, a hierarchical structure is proposed for a scalable network. The hierarchical structure has clusters of sensor nodes based on geographical proximity. Sensor nodes are the set of sensors present in the network, arranged to sense the environment and collect the data. Each cluster has a specially designated node called the cluster head. The function of the cluster head is to perform common functions for all the nodes in the cluster. This hierarchical structure is shown in Figure 1.

Manuscript received October 11, 2008.

A. Abbasi is with the AFTA Center, Tehran, Iran (phone: 935-658-5794).

III. SECURE COMMUNICATION

Security issues related to sensor networks, introduce a rich field of research problems. Improving hardware and software may address many of the issues, but others will require new supporting technologies [4]. Some security mechanisms, are hardware-based and need special hardware circuits, but, with current technology, hardware solutions increase energy consumption and hardware complexity for sensor network.

The security requirements in sensor networks include confidentiality, integrity and authentication. Security consideration at the design time is the best way to ensure successful network deployment. Protocols and software applications should consider security in their original designs. Also, sensor networks, especially with regard to resisting attacks on network availability, must consider security issues in their original design. Attempts to add security afterwards, usually prove unsuccessful.

In hierarchical structure, the fact that only the cluster head is transmitting information out of the cluster, helps saving energy and avoiding the black hole problem [7]. Changing the cluster heads in the hierarchical structure, is a technique that can increase security. The proposed hierarchical structure does not impose any special requirement on the cluster head and it can be any ordinary sensor node in the cluster.

Thus, when the cluster head is fixed, the probability of compromising a link for internal communications (communications between two nodes in the same cluster) is

$$p_{\text{inter}} = \begin{cases} \dfrac{N_{comp}}{N_{CH}} & N_{comp} < N_{CH} \\ 1 & N_{comp} \geq N_{CH} \end{cases} \quad (1)$$

N_{CH} and N_{comp} are the number of cluster heads and the number of compromised nodes, respectively. The probability of compromising a link for external communications (communications between two nodes in different clusters) is

$$p_{exter} = \begin{cases} \dfrac{2N_{comp}}{N_{CH}} - (\dfrac{N_{comp}}{N_{CH}})^2 & N_{comp} < N_{CH} \\ 1 & N_{comp} \geq N_{CH} \end{cases} \quad (2)$$

These probabilities are shown in Figure 2, for $N_{CH} = 30$. We see that the probabilities will be equal to one, when the number of compromised nodes is greater than the number of cluster heads.

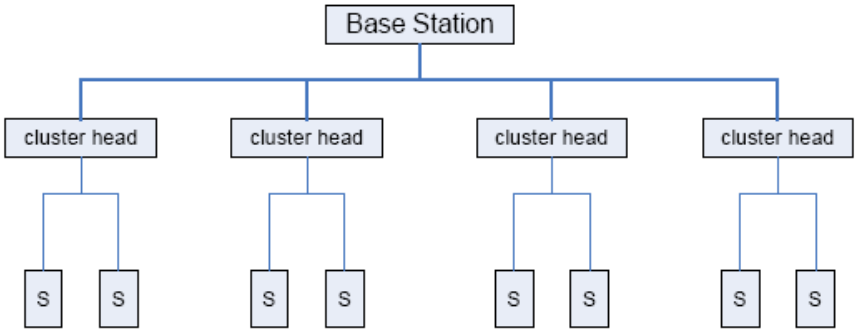

Figure 1. hierarchical structure

In such a situation, network communications will be extremely unsecure. For this problem, changing the cluster heads periodically can be a proper solution. In this situation, it is assumed that the period of rotation of the cluster heads is smaller than a finite amount of time that an attacker can compromise a node. Thus, if the number of sensor nodes is N, the probability of p_{inter} and p_{exter} are approximately

$$p_{inter} = \frac{N_{comp}}{N} \tag{3}$$

$$p_{exter} = \frac{2N_{comp} - 1}{N} - \frac{(N_{comp} - 1)N_{comp}}{N^2} \tag{4}$$

These probabilities are shown in Figure 3, for $N = 1000$. We see that the idea, considerably improve security for both external and internal communications, but unfortunately this method increases complexity of the security protocols.

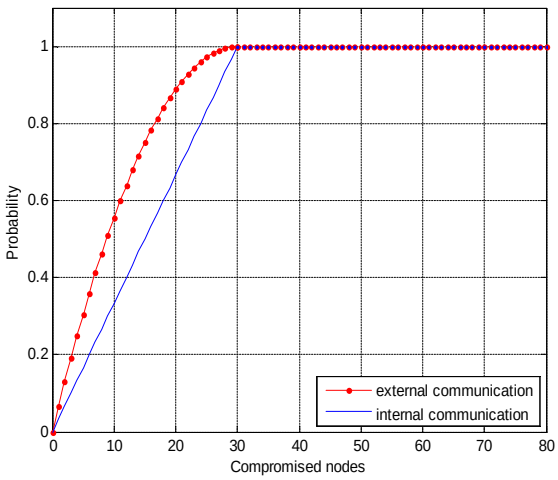

Figure 2. The probability of compromising a link for fixed cluster heads

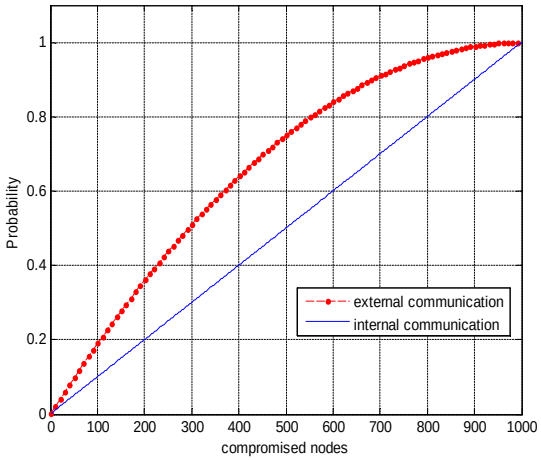

Figure 3. The probability of compromising a link for rotational cluster heads

IV. ENERGY CONSUMPTION

The most important constraint that affects on wireless sensor network capabilities is power consumption. In a wireless sensor network, a sensor neither can be replaced nor can be recharged. Therefore, to increase security lifetime, sensor power should be maintained.

Now, if we want to add a cryptographic protocol to a sensor node, we should consider its effects against network limited energy. Thus, energy consumption is essential to be considered when designing a security protocol.

V. THE PROPOSED SECURITY PROTOCOL

At first, a key distribution protocol is proposed. Every node is associated with a cryptographic key (Figure 4). Every node has a unique index. Each sensor node gets all keys of children of its parent and also all keys of its parent level (except its parent key) and so on. In this protocol, for communication between two nodes, the key that is common between these two nodes, is used.

A probabilistic key distribution is also used to compute Message Authentication Codes. In this probabilistic key distribution, each sensor node selects randomly n keys among m keys that a sensor network possess.

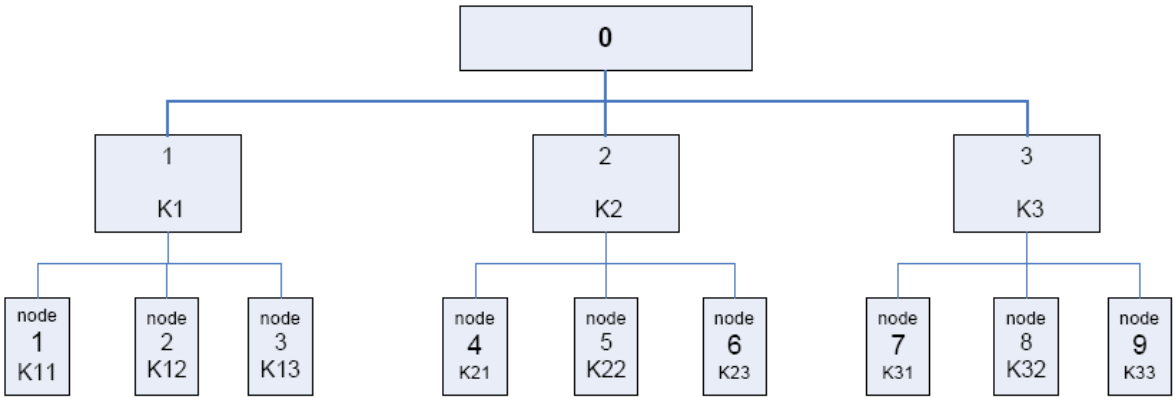

Figure 4. a key distribution protocol for sensor network

After the keys are assigned to the sensor nodes, we settle them into the sensor field. It is assumed that the total number of keys is m and the total number of keys that belong to each sensor node is n. When a sensor node sense an event, it generates a message with following format

$T|E|i1|M_{i1}|i2|M_{i2}|i3|M_{i3}|\ldots|ih|M_{ih}$

that in which,
T: message time
E: data
i1,i2,…,ih: indexes of Message Authentication Codes
M_{i1}, M_{i2}, …: Message Authentication Codes

and sends it to other sensor node.

It is considered that for any message, h number of keys is selected randomly from m keys of a sensor node and these selected keys are used to compute h number of MACs. These MACs and corresponding key indexes are attached to a message. We assume that a message is not transmitted in the following situations: the number of MACs is less than h, and one key is used more than once.

As it was described previously, h number of MACs is used in the proposed protocol. We assume that an attacker possesses g number of h keys. So, he has to possess other h-g keys. If the probability that he has one of the h-g keys is p, then

$$p = 1 - (1 - \frac{h-g}{m})^n \qquad (5)$$

The probability that a message, after i hop, is detected as false data is

$$p_i = 1 - (1-p)^i \qquad (6)$$

False data detection probabilities shown in Figure 5, for $m = 800$, $n = 30$ and $h = 5$. We see that for 10 hopes, in worse situation, 70 percent false data is detected by the proposed protocol.

Now, we analyze our security protocol in aspect of energy consumption. We define

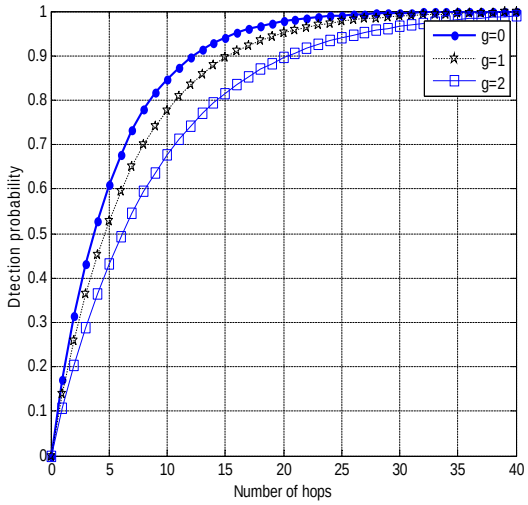

Figure 5. False data detection probabilities

l_{mac} **:** MACs length
l_{index} : index length
l_{data} : data length
E_{mac} : required energy for MAC computation (RC5 algorithm)
E_t : required energy for data transmission per byte
E_r : required energy for receive data per byte
The values of E_{mac}, E_r and E_r is as follows [8]:
$E_{mac} = 16\,mj$, $E_t = 17\,mj$, $E_r = 13\,mj$.
Therefore, the message length before and after applying the security protocol (respectively l_1 and l_2) is

$$l_1 = l_d \qquad (7)$$

$$l_2 = l_d + l_{mac} + h \times l_{index} \qquad (8)$$

Assume that the number of message hops is i, and the number of false message is F. Therefore, energy consumption before and after applying the security protocol (respectively E_1 and E_2) is

$$E_1 = l_d \times (E_t + E_r) \times (F) \times i \quad (9)$$

$$E_2 = l_2 \times (E_t + E_r) \times (F \times (1-(1-p)^i) \times p^{-1}) + h \times E_{mac} \times F \times (1-(1-p)^i) \times (p^{-1}) \quad (10)$$

Equations 5 and 10 indicates that, for obtaining maximum security and minimum energy consumption, we must have

$$\begin{cases} (1-p)^i \to 0 \\ \dfrac{1-(1-p)^i}{p} \to 0 \end{cases} \quad (11)$$

and or precisely

$$\begin{cases} (1-p)^i \to 0 \\ \dfrac{1-(1-p)^i}{2p} \le 1 \end{cases} \quad (12)$$

If $i = 25, l_{data} = 32$ bytes, $l_{mac} = 8$ bytes and $l_{index} = 12$ bits,
then the values of energy consumtion are simply computed using equations 9 and 10. The results of these computations are shown in Figure 6.

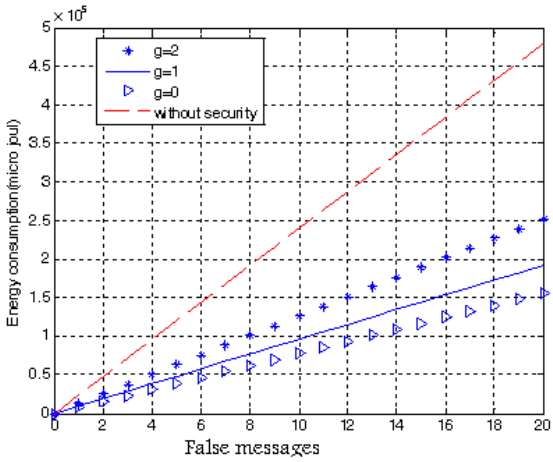

Figure 6. Energy consumption, with and without the security protocol

In this protocol, any sensor node has specific probability for obtaining at least one of the keys that are used in MACs generation. Therefore, a sensor node can verify integrity of the MACs that are attached to the message. If an attacker obtains one key, he can generate only one correct MAC.

When a sensor node receives a message, it operates according to the following process:

A. It computes the number of indexes and MACs. If the number of them isn't equal, the message is detected as false data and it is dropped.

B. If the number of indexes and MACs are equal, it computes a MAC using its key and compares it with the message's MAC. If they are same, the message is forwarded to the next node. Otherwise, it is dropped.

C. If it hasn't any key that is used in computation of the message's MACs, the message is forwarded to the next node.

VI. SIMULATIONS

We simulated the proposed protocol using NS-2. Simulation is done on a square 3600 m^2 area. In this area, we distributed 400 nodes uniformly. Any node has 30 keys and the total number of network keys is 800. the results of simulation are shown in Figures 7 and 8. These results confirm the straightforward mathematical analysis done in section V.

This protocol, when the number of hops is great, improves sensor node and network lifetime and prevents additional energy consumption as well as increasing security.

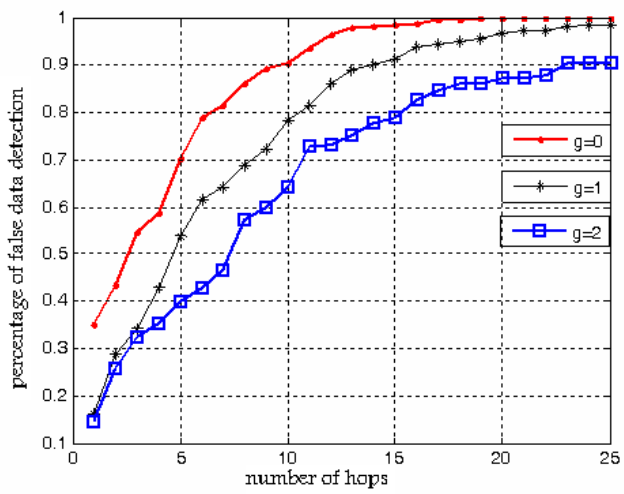

Figure 7. false data detection

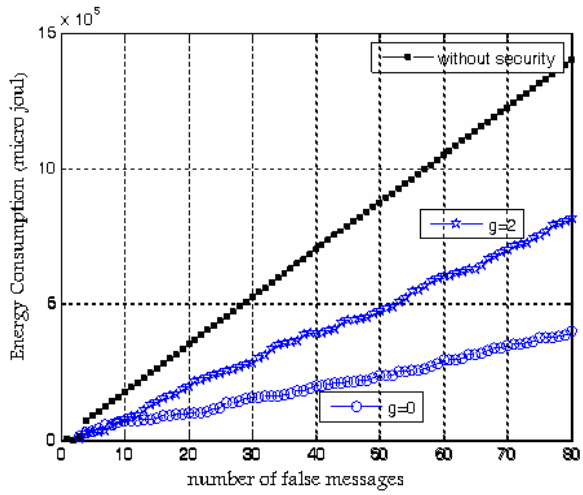

Figure 8. energy consumption, with and without the security protocol

VII. SECURITY LEVEL SELECTION

Now, we can compute basic parameters of the proposed protocol (i.e. m, n or h) using equations 5 and 6. For example, if we expect a false message is detected after 4 hops and with $p_i = 0.9$, we must have (using equation 6):

$p = 0.56$

if we suppose $h = 5$ and $g = 2$, then we must have (using equation 5):

$\frac{m}{n} \approx 6$

Therefore, in this example, the number of each sensor node keys must be at least $\frac{1}{6}$ of the total number of keys. Because of $i = 4$ and $p = 0.56$, lower energy consumption is also provided.

Thus, the proposed protocol provides a security-level selection mechanism and therefore, it is better than SPINS protocol. The SPINS protocol has a binary security mechanism –either has maximum security or no security [9].

VIII. APPLICATIONS

Due to special characteristic of the proposed protocol, it can be used in military applications. In military areas, an attacker tries to inject false messages into a sensor network in order to insert false information or decrease the network trust. Furthermore, this action results in additional energy consumption for a sensor network and decreases its lifetime. Thus, the proposed protocol can be a security solution against these attacks.

IX. CONCLUSIONS

Providing sensor network security is a very important issue. Lack of security, in addition to reveal secret information, decreases the lifetime of these networks in many cases. The security protocol that is proposed in this paper, in addition to increase security, results in lower energy consumption for a sensor network. This security scheme prevents energy exhaustion attacks and thus increases network lifetime. On the other hand, it can provide a special security level based on desirable data protection.

REFERENCES

[1] Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Communications Surveys, 2nd quarter 2006, vol. 8, No. 2.
[2] I. F. Akyildiz et. al., "A Survey on Sensor Networks", IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp. 102-114.
[3] E. Shi and Perrig, "Designing Secure Sensor Networks", Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004, pp. 38-43.
[4] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks", IEEE Comp. Mag., Oct. 2002, pp. 103-105.
[5] D. W. Carman, P. S. Kruus, and b. J. Matt, "Constraints and Approaches for Distributed Sensor Network Security", Technical Report #00-010, NAI Labs, 2000.
[6] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks", IEEE Comp. Mag., Oct. 2002, pp. 54-62.
[7] M. L. Arboleda C. and N. Nasser,"Comparision of clustering algorithms and protocols for wireless sensor networks", IEEE, May 2006.
[8] Cross Bow Technologies, website: http://www.xbow.com/.
[9] A. Wadaa et al.,, "A Scalable Solution for Securing Wireless Sensor Networks", Book chapter in Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless and Peer-to-Peer Networks, editor: Jie Wu, Auerbach Publications, 2006.