International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:5, No:5, 2011

Securing Message in Wireless Sensor Network by using New Method of Code Conversions

Ahmed Chalak Shakir, GuXuemai, and Jia Min

***Abstract*—**Recently, wireless sensor networks have been paid more interest, are widely used in a lot of commercial and military applications, and may be deployed in critical scenarios (e.g. when a malfunctioning network results in danger to human life or great financial loss). Such networks must be protected against human intrusion by using the secret keys to encrypt the exchange messages between communicating nodes. Both the symmetric and asymmetric methods have their own drawbacks for use in key management. Thus, we avoid the weakness of these two cryptosystems and make use of their advantages to establish a secure environment by developing the new method for encryption depending on the idea of code conversion. The code conversion's equations are used as the key for designing the proposed system based on the basics of logic gate's principals. Using our security architecture, we show how to reduce significant attacks on wireless sensor networks.

Keywords—logic gates, code conversions, Gray-code, and clustering.

I. Introduction

RECENTLY, wireless sensor networks have become a hot technological topic with the development of computer science and wireless communication technology. Sensor nodes are deployed in a hostile or unattended environment to collect the data information [1]. They will play a key role in future smart environment. 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 [2]. Wireless networks in general are more vulnerable to security attacks than wired networks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected [3]. For the applications, particularly for wireless devices in which the potential for attackers is seen as greater, security will be demanded. So, security issues related to sensor networks introduce a rich field of research problem. The security requirements in WSNs include: *Confidentiality* means to ensure that information contained in the data is only disclosed to users or devices for which the data was intended. This can be achieved by encrypting the data. *Authentication* means to ensure that a receiver of the data is able to check whether the data originate from the claimed sender or not. *Reply protection* means to ensure that an attacker is not able to record a message and send it successfully to a node at a later point in time. It can be achieved by adding unique information to each message. The simplest way is to add the current number of a computer to the message and increase it afterwards. Hence each message contains a unique sequential number [4]. To achieve security in WSNs, it is important to be able to encrypt and authenticate messages sent among sensor nodes and this is what we achieved in our system. The heterogeneity among sensor nodes helps provide scalability, notable energy efficiency and security benefits. To exploit these advantages, we consider a two-layered (tiered), heterogeneous (which refers to networks consisting of a large number of resource-constraint sensor nodes used for data measurements and fewer resource-rich wireless devices that can be used for complex computations, decision making, and data relaying) sensor network when designing the proposed key management protocol[5].

F. Ahmed Chalak Shakir is a PhD candidate with the Harbin Institute of Technology, School of Electronics and Information Technology, Harbin, Heilongjiang, China (phone: 008615114551049; e-mail: ahmedchalak@ hit.edu.cn).

S. Professor GuXuemai , with the Harbin Institute of Technology, School of Electronics and Information Technology, Harbin, Heilongjiang, China (e-mail: guxuemai@ hit.edu.cn).

T. Dr. Jia Min , with the Harbin Institute of Technology, School of Electronics and Information Technology, Harbin, Heilongjiang, China (e-mail: jiamin@ hit.edu.cn).

II. Related work

Key management poses a main concern for security operation in sensor networks. Many key management protocols are proposed for homogeneous sensors networks. However, these networks have limited performance and security. Heterogeneous sensor networks are proposed to outcome these drawbacks [5]-[9].

Ashok Kumar et al [11] considered an HWSN that consisted of two types of sensors: a small number of powerful High-end sensors (H-sensors) and a large number of resource-constrained Low-end sensors (L-sensors). H-sensors can execute relatively complicated numerical operations and have a much larger radio transmission range and storage space than L-sensor nodes. On the other hand, L-sensors are extremely resource-constrained. Prevention of injection packets and old messages replication previously delivered are not considered. Chung-Horng [10] has shown that in WSNs, Hierarchical network which is considered in our study provide better performance in scalability, self-organization, and energy efficiency than homogeneous networks. Wensheng Zhang et al [12] considered that due to high computational and communication overhead, the digital signature-based authentication techniques are not suitable for sensor networks.

In our paper we considered a new light technique for using the signature with very small computational overhead. Samuel Pierre et al [13] considered that clustering has been proven to be energy efficient in sensor networks since data routing and relaying are only operated by cluster heads that can process,

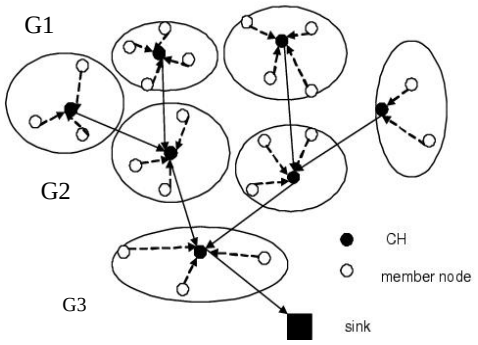
filter and aggregate data sent by cluster members, thus reducing network local and alleviating the bandwidth.

III. Clustering in General

Wireless sensor networks (WSNs) have attracted significant attention over the past few years. A growing list of civil and military applications can employ WSNs for increased effectiveness, especially in hostile and remote areas. Examples include disaster management, border protection, and combat field surveillance. In these applications a large number of sensors are expected, requiring careful architecture and management of the network. Grouping nodes into clusters has been the most popular approach for support scalability in WSNs [14]. The clustering consists of a virtual division of the network in groups of nodes geographically close. In a typical cluster structure, every node plays a specific role such as cluster-head or cluster-gateway or cluster-member. The cluster-head normally is in charge of the local managing of the cluster, performing the arrangements of the intra-cluster communication, data forwarding and more. The cluster-gateway disposes an inter-cluster link to forward data to a neighbor cluster. The cluster-member is just an ordinary node in the cluster [15]. Finally, the energy-efficiency in clustering sensor networks has been proven in [16]-[18].

IV. Hierarchical Structure

Generally there are two different architectures (planner and hierarchical) of WSN. Planner or flat is easier for deployment while hierarchical structure is simpler to implement [19]. For a scalable network the hierarchical structure is proposed, which has clusters of sensor nodes based on geographical coming closer of the nodes. Each cluster has a special designated node that performs common functions for all the nodes in the cluster called cluster head as shown in the figure 1.



Clustering Structure in Groups

V. System codes and Conversions

A code is a rule for converting a piece of information (for example, a letter, word, phrase, or gesture) into another form or representation (one sign into another sign), not necessarily of the same type. In communications and information processing, encoding is the process by which information from a source is converted into symbols to be communicated. Decoding is the reverse process: converting these code symbols back into information understandable by a receiver. In digital communication all the information is represented by binary numbers, which are either 0 or 1. Many coding systems exist for communication, and each one has its own use depending on the applications like EX-3 code, EBCDC code, gray-code, and so forth. There is also the ability to convert from one system code to another depending on the need.

VI. Assumption

The following assumptions are considered in our study:

1. Static sensor network is assumed, where all sensor nodes have fixed locations.
2. The BS (base station), acting as a sink, is trusted and will never be compromised. It is equipped with tamper-resistant material.
3. H-sensors are equipped with tamper-resistant hardware to protect their supplementary keying materials from compromise. In addition, intrusion detection systems should be integrated in H-sensors to detect malicious behavior, since H-sensors are powerful nodes. Each H-sensor preserved the pair of signature and ID of each sensor connected to it.
4. An L-sensor communicates only with H-sensors and never with another L-sensor. For precision, each L-sensor can establish a link with only two H-sensors, one by default and another as back up in the case where it cannot establish a link with the first. Sensor nodes are organized in clusters, and each node knows to which cluster it belongs.
5. L-sensors are not equipped with tamper-resistant hardware. Thus, if an L-sensor is captured, its contents are considered to be compromised.
6. Each sensor has a unique ID.
7. The word of the “key” in the paper refers to equations generated from the tables of codes prior to deployment.
8. Each L-sensor contains the ID of the CH that communicates with beside of its ID.

VII. Proposed Security System Model

There is a direct relationship between force protection for the information and the complexity of the algorithm used. The more complex algorithm has a large degree of protection and consequently affects the efficiency of the device used.

Therefore, the challenges are many in order to provide very strong protection of information using algorithms with simple survival while increasing the efficiency of the device used (sensors). In the proposed system, many equations are used for getting the stuff working as a key for securing the messages transmitted between:

a) Cluster heads and the nodes belong to them.
b) Cluster head and cluster head.
c) Cluster head and the base station.

These equations are coming from the new codes created during the design process and changed periodically for overcoming the compromised node. Each cluster has its own rules for when and how to change its codes or its equations that are used for securing the messages. To explain the idea, suppose that we have the structure shown in figure1, here CH

is the cluster head and the sink is the base station. There are three communication links in such wireless sensor networks, which are:

a) Between the node and the cluster head inside the same cluster or group.
b) Between Cluster heads, as in between CH in group1 (G1) and the CH in group 2 (G2).
c) Between CH and the BS (base station) or sink, as in between G3 and the sink.

The base station is assumed to be secure and trusted by all the nodes in the network. So, for communication between nodes and the cluster head the following procedure is applied:
In order to find the equations that are used for securing the messages transferred among the overall network; the truth table is used for explanation and producing code conversions. Three variables are taken as shown in table I so that all three bits are processed individually and in sequence. This is very important so that the attacker cannot get the information in the case of node compromising. The $(2^n)!$ tables can be generated without the redundant states, where n is the number of inputs variables. For the example shown in table I, where n=3, then $2^3! = 40320$ tables can be generated.

TABLE I.
TRUTH TABLE OF THREE INPUTS

Decimal	A	B	C
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1

For instance, if two tables are constructed as shown in table II, then the equations that are used for securing or encryption and decryption the message can be illustrated by the following equations:

$$X = \bar{A}.\bar{B}.\bar{C} + \bar{A}.\bar{B}.C + \bar{A}.B.C + A.B.C \quad (1)$$
$$Y = \bar{A}.\bar{B}.C + \bar{A}.B.\bar{C} + \bar{A}.B.C + A.\bar{B}.C \quad (2)$$
$$Z = \bar{A}.\bar{B}.\bar{C} + \bar{A}.\bar{B}.C + \bar{A}.B.\bar{C} + A.B.C \quad (3)$$

By using the karnaugh map for simplification yields:

$$X = \bar{A}.\bar{B} + \bar{A}.C + A.B.C \quad (4)$$
$$Y = \bar{A}.B + \bar{B}.C \quad (5)$$
$$Z = \bar{A}.\bar{C} + \bar{A}.\bar{B} + A.B.C \quad (6)$$

Let *S* be the sender and *R* be the receiver, then *S* is using XYZ for encryption and using ABC for decryption, while *R* is using ABC for encryption and using XYZ for decryption (as mentioned, each ABC or XYZ is a key used for encryption and decryption).

TABLE II.
GENERATING TWO TABLES OF CODES

A	B	C	X	Y	Z
0	0	0	1	0	1
0	1	0	1	1	1
0	0	1	0	1	1
0	1	1	1	1	0
1	0	0	0	0	0
1	1	0	0	1	0
1	0	1	1	0	0
1	1	1	0	0	1

The equations (4, 5, and 6) are used by the sender *S* for securing the message while the receiver *R* uses the equations (10, 11, and 12) for decrypting or getting the original message.

$$A = \bar{X}.\bar{Y}.\bar{Z} + \bar{X}.Y.\bar{Z} + X.\bar{Y}.\bar{Z} + \bar{X}.\bar{Y}.Z \quad (7)$$
$$B = \bar{X}.Y.Z + X.Y.\bar{Z} + X.\bar{Y}.\bar{Z} + \bar{X}.\bar{Y}.Z \quad (8)$$
$$C = X.Y.Z + X.Y.\bar{Z} + \bar{X}.Y.\bar{Z} + \bar{X}.\bar{Y}.Z \quad (9)$$

By using the karnaugh map for simplification yields:

$$A = \bar{X}.\bar{Z} + \bar{X}.\bar{Y} + \bar{Y}.\bar{Z} \quad (10)$$
$$B = X.\bar{Z} + \bar{X}.Z \quad (11)$$
$$C = X.Y + Y.\bar{Z} + \bar{X}.\bar{Y}.Z \quad (12)$$

For more clarifications the virtual logic circuits design shown in figures 2&3 can illustrate the procedure of encryption and decryption by using the new method of code conversions instead of the key.

For the above example,*S* wants to send the following streams of bits to *R* regardless of the meaning at this time:
10101010001100010101010001111110110101010010101010001
Then each of the three bits is isolated so that our code system is for three inputs only as follows:
101|010|100|011|000|101|010|100|011|111|101|101|010|100|101|010|001| then by using XYZ equations yields:
010|011|000|110|101|010|011|000|110|001|010|010|011|000|010|011|111

This stream of bits is encrypted so that it changes its values and be other values (definition of encryption) are return to its original when received by the receiver *R* by using ABC equations. If the number of zeros and ones is not multiplies of 3, then zeros are added at the end of the stream as a pad and manipulated as explained in the above example.

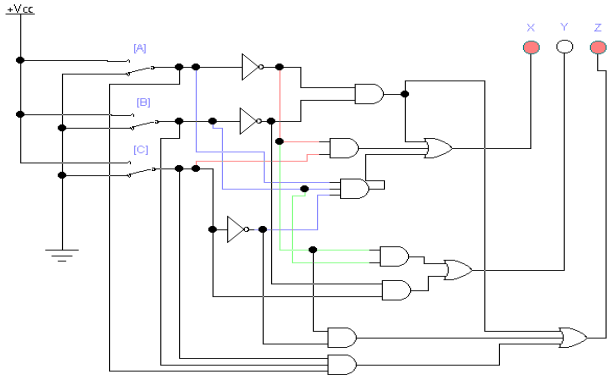


Fig.1. The sender S is using XYZ equations for encryption.

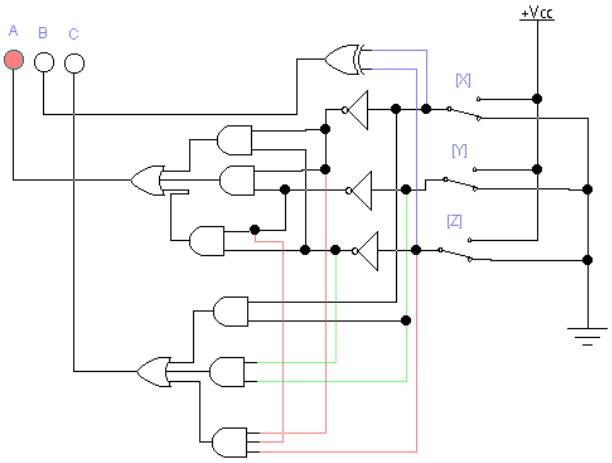


Fig.2. The receiver R is using ABC equations for decryption.

VIII. Inside the Cluster Head

The CH could be regarded as any other sensor to be used for receiving and sending. It contains two type of circuits; one of them is used for receiving (CFR: circuit for receiving) and the other is used for sending (CFS: circuit for sending).

A. CFR

The operations of the receiving circuit for the Cluster head can be illustrated by the flowchart shown in figure 4.

Where:

Control Unit: splits the received signal, which is a combination of sensor signature, message counter and the securing message. Inside the control unit, there is a gray-code system, which converts the first 10-bit of the received signal (signature) from the gray code to the binary number. The result must be the ID of the sensor that sent the signal. That means the ID is gotten from the signature and it didn't send with the signal. Then the signature is compared with the one whose ID is found.

Signature Comparator: gets the signature from the control unit. It contains X-OR gates to make a comparison between the exits signature and the new entered one (whose ID is found earlier). If the result of comparison is equal to zero (rules of Boolean algebra: (A) X-OR (A) = 0), that means the signature is of the intended sensor. But, if the result is not zero, then the signal or the message is neglected.

Message Counter Comparator: it takes the second 10-bit, which represents the message counter and compares it with the last save one for greater than, which is represented by 1, or for smaller than or equal to, which is represented by 0. If the result is greater than the last saved, then it will ANDing with other signal of signature comparator result to notify that the entered message has not duplicated, or else the message is neglected.

Control Signal: it makes the ANDing between the two signals (binary numbers) coming from the comparisons result in a message counter that is always 1 (greater than) and the signature which is either 0 or 1. If the signal from the signature comparator is C1 and from the message counter comparator is C2, then to make the message pass through the tri-state buffer, the input signal must be equal to 0. Which means C1 AND C2 = 1. C2 by default is equal to 0; if C2 equal to 0 then the message will be pass but if C1 =1 then C1 AND C2 =1, which means high impedance of tri-state buffer and the message will be neglected because the signature is not for intended sensor.

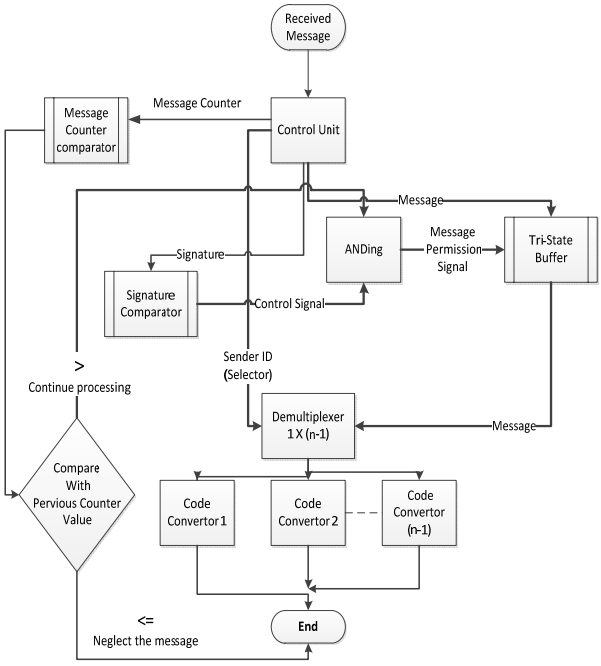


Fig.3. Flowchart circuit for receiving secured message.

Tri-state buffer: (active-low control line, works by zero input and needs low energy), which gets the signal from the control signal and works as shown in table III.

TABLE III.
Tri-state buffer

Control	Input	Output	Comment
1	X	High impedance	Output (No)
0	0	0	Output (Yes)
0	1	1	Output (yes)

If the control signal is 1, then received message wouldn't be passed to another circuit (neglected) so that is not from the intended sensor, but if the control signal value is 0 then the message is passing to the Demultiplexer circuit.

De-multiplexer: gets the selector from the control unit, which is the ID of the sender sensor and got by gray-code (signature). It is used to decide which code conversion circuit the secured message should be used for getting the original message.

Code Conversion circuit: each senor has an ID, and according to its ID the circuits of code conversions are designed in the cluster head so that it is used for decryption or getting the original message.

B. CFS

The operation of the sending part for the CH can be illustrated by the figure 5.

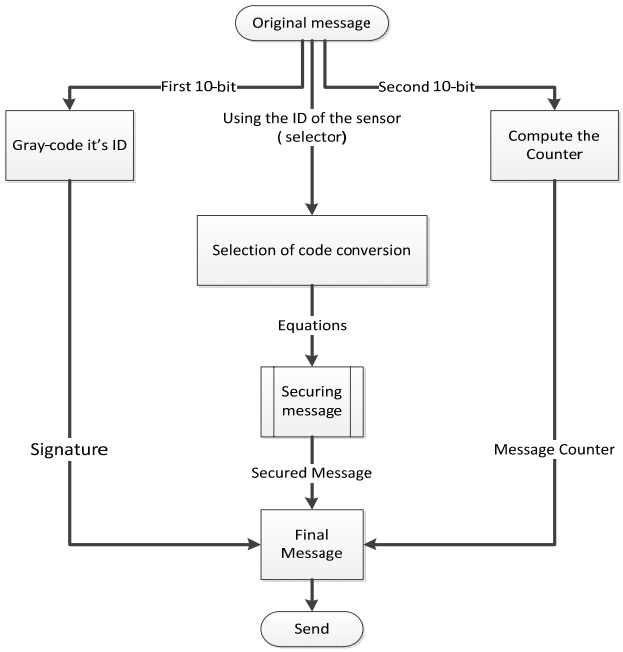


Fig.4. Flowchart circuit for sending the secured message

Where:
Gray-Code its ID: takes the first 10-bit of the original message (original message organized as ID, counter, and the message) and converts it to Gray-code to produce the signature of itself.
Compute the Counter: gives the numerical value to the current message, which represents its sequence from the overall message that would be sending.
Selection of Code Conversion: according to the ID of the sensor to be sending to, the decision would be made for which equations (Code) to be used. Each sensor has its own equations used for encryption and decryption preserved in the CH and also in the L-sensor.
Securing Message: using the equations that are selected from the previous step for securing the message as discussed in the example of section VII.
Final Message: the whole message including the signature, message counter and the encrypted message is sent to either other CH in the network or to the L-sensor in its cluster group.

IX. Inside the L_sensor

Each node contains two circuits; one of them is used for sending and the other is used for receiving.

A. Receiver Circuit

The receiver circuit of the L-sensor is illustrated in figure 6.
Where:
Control Unit: splits the whole message, which is encrypted message, signature and the message counter. Each one of them enters into its own process circuit.
Gray-code Conversion: gets the signature, which is in Gray-Code format, and converts it to its original binary code. The result is the ID of the CH that sent the message. The ID of such cluster head is preserved in the L-sensor.
ID Comparison: makes a comparison between the ID gotten from the previous step and the preserved one of such CH node. If the result of comparison is 0, that means they are matched (rules of Boolean algebra: (A) X-OR (A) = 0) and can be a control signal used with other control signal on the tri-State buffer for making the encrypted message be passed, else the message is neglected.

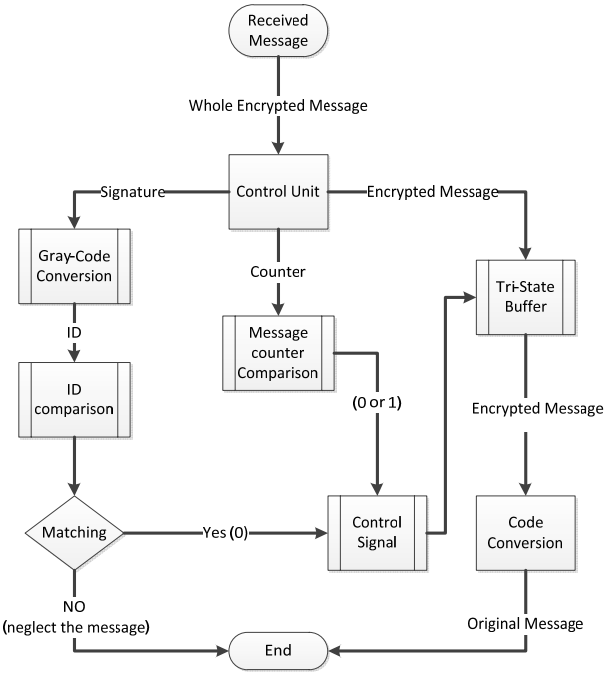


Fig.5. Flowchart of receiver circuit of the L-sensor

Message Counter Comparison: makes a comparison with the previous message sent from the same CH for greater than, which is represented by 1 and for smaller than or equal to, which represented by 0. The result signal is combined with the signal from ID comparison.
Control Signal: combines the signals (bits) from the ID and message counter comparison. It has the equation of (Z=A`. B`) where A is the bit from the ID comparison and always equal to 0, and B is the bit from the message counter comparison and may be equal to 0 or 1. Regard that the tri-state buffer is working and passes the message if the result bit of control signal is equal to 0. The states are shown in table IV.
Tri-State Buffer: (active-low control line, low energy needs to work). Pass the encrypted message to the code conversion process when the bit from the control signal process is equal to 0.
Code Conversion: apply its own equations to decrypt the message and get the original message.

TABLE IV
CONTROL SIGNAL STATES

A	Meaning	B	Meaning	Z	Meaning
0	The matching is done between two IDs	0	The result of comparison is smaller than or equal to the previous one (duplicated message)	1	The message be neglected and not passed to the next step
0	The matching is done between two IDs	1	The result of comparison is greater than the previous one	0	The encrypted message will be pass to the next step
1	Never happened	0	The result of comparison is smaller than or equal to the previous one (duplicated message)		----
1	Never happened	1	The result of comparison is greater than the previous one		----

B. Sender circuit

The sender circuit of the L-sensor is illustrated in figure 7. Where:

Gray-Cade its ID: takes the ID and converts it to Gray-code to produce the signature.

Securing Message: encrypts the message, by using the equations of code conversion preserved in the sensor.

Compute the Counter: gives the sequence number of the sending message.

Final Message: collects all the information, which is the signature, counter and the encrypted message respectively, then sends the whole message to the H-sensor.

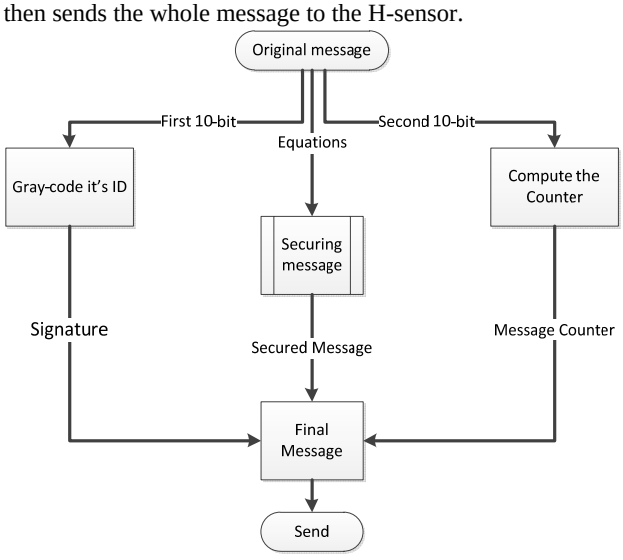


Fig.6. Flowchart of sender circuit of the L-sender

X. Discussion and Security Analysis

Usually, cryptosystems are used to protect the data confidentiality and integrity, including symmetric and asymmetric encryption algorithms. But applying them to wireless sensor networks is always a debatable topic due to the limitations and disadvantages of these algorithms. In our paper we develop a new method for designing the security architecture and can efficiently protect the message. We can summarize the method and its advantages by the following points:

a) The Gray-code is used for producing the signature from the ID of the sensor. Compared with another method for producing a signature like elliptic curve cryptography (ECC), our method is less power consumption and very light, especially for L-sensor, which has many restrictions. This is a type of authentication that exists in the system.

b) The compromised node doesn't affect the other nodes in the cluster group so that each L-sensor has its own code conversion equations and from the compromised one the code conversion equations of other nodes cannot be extracted.

c) Confidentiality was proved in our system by encrypting the message using the code conversions as a key.

d) By using the message counter the reply protection is done so that an attacker is not able to record a message and send it successfully to a node at a later point in time.

XI. Conclusion

Building secure sensor networks is of paramount importance, but it is quite difficult; for that reason there is a tradeoff between the security strength and the complexity of the proposed solution for protecting the message from eavesdropping. In this paper we solved the problem of messages security transferred among sensors until they reached safely to the base station and developed security architecture in WSN with heterogeneous sensor nodes. The new method is used by exploiting the idea of code conversions with the Gray-code system to encrypt the whole message.

Acknowledgments

Authors would like to thank Harbin Institute of Technology, School of Electronics and Information Technology, China, for supporting this work research.

References

[1] Shuai Yang, Jie Liu, Chunxiao Fan, Xiaoying Zhang, and JunweiZou. "A new design of security wireless sensor network using efficient key management scheme". IEEE, DOI: 10.1109/ICNIDC.2010. 5657820, Issue Date: 24-26 Sept. 2010.

[2] Akbar Abbasi, "Better Security for Wireless Sensor Networks," icfn, IEEE, pp.100-103, International Conference on Future Networks, 2009. http://doi.ieeecomputersociety.org/10.1109/ICFN.2009.55

[3] XiuliRen, and Haibin Yu, "Security Mechanisms for Wireless Sensor Networks". IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.3, March 2006

[4] Beat Gebistorf and Roger Wattenhofer. "Secure Messaging for Wireless Sensor Networks". Swiss Federal Institute of Technology Zurich, Distributed Computing Group DCG. Semester thesis, SA-2009-03.

[5] ManelBoujelben, Omar Cheikhrouhou, Mohamed Abid and Habib Youssef. "Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks". Third International Conference on Sensor

Technologies and Applications. 978-0-7695-3669-9/0 IEEE DOI 10.1109/ SENSORCOMM.2009.73

[6] Kejie Lu, Yi Qian and Jiankun Hu. "A Framework for Distributed Key Management Schemes in Heterogeneous Wireless Sensor Networks". IEEE 1-4244-0198-4/06©2006

[7] Jen-YanHuang, I-En Liao, and Hao-Wen Tang. "A Forward Authentication Key Management Scheme for Heterogeneous Sensor Networks". Hindawi Publishing Corporation.EURASIP Journal on Wireless Communications and Networking Volume 2011, Article ID 296704, 10 pages. doi:10.1155/2011/296704.

[8] Reza Azarderakhsh, ArashReyhani-Masoleh, and Zine-EddineAbid. "A Key Management Scheme for Cluster Based Wireless Sensor Networks". IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. 978-0-7695-3492-3/08 IEEE. DOI 10.1109/EUC.2008.176

[9] Zhong Zhou, Student Member, IEEE, Shengli Zhou, Member, IEEE, Shuguang Cui, Member, IEEE, and Jun-Hong Cui, Member, IEEE. "Energy-Efficient Cooperative Communication in a Clustered Wireless Sensor Network". IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 57, NO. 6, NOVEMBER 2008

[10] Chung-Horng Lung and Chenjuan Zhou. "Using Hierarchical Agglomerative Clustering in Wireless Sensor Networks: An Energy-Efficient and Flexible Approach". 978-1-4244-2324-8/08/, IEEE 2008.

[11] Ashok Kumar Das and IndranilSengupta. "An Effective Group-Based Key Establishment Scheme for Large-Scale Wireless Sensor Networks using Bivariate Polynomials". Conference: COM-munication System softWAre and Middle-waRE - COMSWARE , pp. 9-16.DOI: 10.1109/ COM-SWA.2008.4554370.

[12] Wensheng Zhang , Sencun Zhu ,and Guohong Cao. "Predistribution and local collaboration-based group rekeying for wireless sensor networks". Ad Hoc Networks 7 (2009) 1229–1242. 2008 Elsevier B.V. All rights reserved. doi:10.1016/j.adhoc.2008.11.004

[13] Ali Chamam and Samuel Pierre. "A distributed energy-efficient clustering protocol for wireless sensor networks". Computers and Electrical Engineering 36 (2010) 303–312. doi:10.1016/j. comp eleceng.2009.03.008. 2009 Elsevier Ltd.

[14] Ameer Ahmed Abbasi and Mohamed Younis. "A survey on clustering algorithms for wireless sensor networks". Computer Communications 30 (2007) 2826–2841. doi:10.1016/j.comcom.2007.05.024. _ 2007 Published by Elsevier B.V.

[15] Renaud Fallier and Bart Scheers. "Positioning and Topology Control in Mobile Ad Hoc Networks and Wireless Sensor Networks". NC3A (Den Haag) and the VUB / ETRO-COMO 2011. http://www.sic.rma.ac.be/Projects/WSN/index.html

[16] Arboleda LMC, Nasser N. "Comparison of clustering algorithms and protocols for wireless sensor networks". In: Proceedings of the Canadian conference on electrical and computer engineering; 2006. p. 1787–92.

[17] Heizelman WR, Chandrakasan A, Balakrishnan H. "Energy-efficient communication protocol for wireless micro sensor networks". In Proceedings of the IEEE Hawaii international conference on system sciences; 2000.

[18] Younis O, Fahmy S. HEED. "A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks". IEEE Trans MobileComput 2004;3(4):366–79

[19] SomanathTripathy. "Tin-Key: Effective Key-Establishment for Wireless Sensor Networks". 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010). DOI 10.1109/CIT.2010.170