Tikrit Journal of Pure Science 22 (6) 2017 *ISSN: 1813 – 1662 (Print)*
E-ISSN: 2415 – 1726 (On Line)

Cluster forming based on spatial information using HMAC in WSN

Aso Ahmed Majeed
Public Health Dept. ,Veterinary Medicine Faculty , Kirkuk University, Kirkuk , Iraq
asoalsalihi@gmail.com

Abstract
The wireless sensor can be considered as one of the most major technologies through using it in different application such as environmental applications, military applications, commercial applications, health applications and agriculture applications. Due to the sensor networks may be deployed in open area (uncontrolled area), especially in military applications. In such situations, the nodes are vulnerable to be captured. Moreover, data/control packets may be intercepted and/or modified due to the transmission nature.
Consequently, security services such as authentication and encryption done by key management which is not trivial task. The key management is important to maintain the network operations. The proposed scheme the nodes based on spatial information with data sequence then sends encryption message to each other in secure way by HMAC for providing safe links between the nodes in the network and forming the clusters. Consequently, the proposed scheme covers the security goals and authentication of each node.

Keywords: Heterogeneous WSN, Symmetric Key cryptography, SHA-1, MAC, Attack in WSN.

Introduction
The wireless sensor has become an essential component of modern life and its technologies have seen great development in the last decade. Moreover, Wireless Sensor Networks (WSNs) are used in many applications such as monitoring, target tracking and military applications. However, because the sensors resources are constraint; providing security services in sensor networks and cover the security goals are not trivial problem [1].
There are two kinds of key cryptography: First, Symmetric key cryptography uses a single key, called a secret, which is used to encrypt and decrypt a message by the sender and receiver. In this sense, the sender and the receiver share the same secret key to exchange encrypted messages and to be able to decrypt them [2].
Second, Asymmetric key, the sender/ receiver have their own private keys, which are secrets, and a public key which is known to all nodes in the network. Furthermore, the sender/receiver use both the secret and the public key for encryption and decryption [3].
Secure Hash Algorithm 1 (SHA-1) cryptography which is a type of symmetric key cryptography and it is an essential component of modern cryptography. Furthermore, it is defined as a deterministic procedure that generates a fixed-length bit string, called a digest. In Hash function cryptography, a message with any-length bit string is executed by taking inconstant bit patterns as an input, which then produces constant bit patterns of output. Subsequently, it is interesting to observe for an output message as it computes a unique *digest* [4, 5] as shown in figure 1.

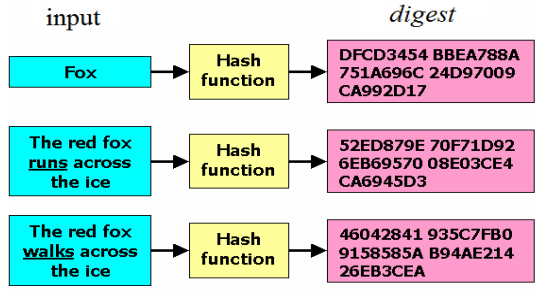

Figure 1 Hash function cryptography

Related work
An important element in the cryptosystem is the key and managing this key in the way of generation and distribution between the nodes in the network is not a trivial task. Furthermore, it has become a hot topic. Key management, therefore, is basic to confirm the security of communication of a wireless sensor network. Henceforth, how to establish an efficient key management in a WSN is a basic challenging problem due to the energy constraints, memory and computational processing capabilities of the sensor nodes [6].
Eschenauer and Gligor proposed the basic probabilistic key predistribution, in each sensor is apportioned a random subset of keys from a key pool before the deployment of the network in pre-distribution phase [1] In this scheme in pre-distribution phase, the two sensors can have a certain probability to share at least one key. Besides, each of them assigned more than one to communicate with other nodes that lead to save more key in their memories. Therefore, the nodes memory exhausted. Moreover, if the adversary captures each node he can get all keys which are assigned to the node. Chan and et al. in [7] developed the *q*-composite key pre-distribution schemes. The *q*-composite key pre-distribution scheme is based on the basic probabilistic scheme in [1], but it requires two sensors share at least *q* pre-distributed keys to establish a pairwise key. In this scheme in pre-distribution phase still assign number of keys (*q*) in each sensor that lead to exhaust their memory. Also, if the enemy arrests each node he can catch the *q* of keys which are allocated to the node. W. Heinzelman and et al. in [8] proposed the LEACH protocol, where the nodes in the network are homogenous (each node has identical characteristics). After deployment, the sensors elect themselves to be the Cluster Head (*CH)* at any given time with a certain probability, after which they then broadcast their status to other nodes within the network. Other nodes select the *CH* sensor according minimum communication energy. In this scheme each nodes work as *CH* periodically that

mean the sensor cost will be expensive because its properties larger than normal node.

In [9] the author's scheme produced to provide the safe links between the nodes in the network and forming the clusters. The Elliptic curve EC is used for generating the seed keys of the pool. Since, the doubling and addition operations for Elliptic Curve (EC) points are used for generating the ring of the private keys. Moreover, EC has many operations for doubling and adding; therefore, the EC is not convenient for cryptography in WSN causes using more energy and exhaustion the sensor resources.

The MAC function is a type of symmetric key cryptography. It meets different security requirements, resists existential bogus plaintext attacks and confirms that the data has not been changed. Consequently, it does not allow malicious nodes to join the network through exchange messages within the network. In addition, it supports data authentication and integrity.

Security goals

In each research, the analysis on security is an essential part. This proposed scheme has also been analyzed to reach the suitable level of security. The achieved securities in this scheme according to some fundamental terms of security are given below.

1- **Authenticity**

Authentication enables each node in the network to ensure the identity of the peer nodes, which communicate with each ot-her so as to eliminate any fake messages and to guarantee that messages come from a trusted node. Symmetric Key Cryptography (SKC) or Public Key Cryptography (PKC) and also the Message Authentication Code (MAC) are utilize to achieve data and node authentication [10].

2- **Confidentiality**

Confidentiality is an important stage to pr-otect and keep any data secret during transmission between sensors and also between Base Station (*BS*) and sensors within the network by concealing messages and then avoiding the enemy. Unauthorized sensors cannot understand the messages, therefore, they remain secret. This is achieved with cryptography [10].

3- **Integrity**

Integrity is of utmost importance to protect the data of received messages from alteration and modification by malicious nodes or adversaries. Until the network has confidentiality, there is still a possibility that data integrity or the message containing the data have been compromised by alterations or change. Integrity stops a malicious node present in the network from injecting bogus data. For this reason, MAC or Hash MAC (HMAC) is used to verify integrity

4- **Availability**

Availability ensures the survivability of sensor network services to authorized parties even though there are attacks within the network. It also ensures the updating of the security mechanism and is not influenced and bordered on the network performance [11].

5- **Freshness**

Freshness ensures that all data and messages exchanged are modern and prevent the resending of old data. To prevent old messages from being sent again by an attacker, a timestamp can be added to the packet to achieve data freshness [11].

6- **Resilience**

The number of keys which an attacker gains by physically capturing some nodes is used by the attacker to hack the whole network and fail the system [12]. The proposed scheme uses tamper resistance to solve this problem.

7- **Scalability**

Scalability means that network size is flexible and its size can increase after deployment, which also ensures the level of security, stability and node properties wh-en increasing the size of the network [11].

8- **Connectivity**

Connectivity is the proportion of the probability of the nodes that are in contact with each other to create a network after deployment in order to ensure better performance of the network. In addition, whenever the percentage of connectivity is hig-her, the quality of network performance is finest [2].

Attacks in WSN

Due of any lack of security, attackers can intercept and read the content of any message. In addition, they can introduce false messages into the system via the network. Moreover, an attacker can capture a sensor and physically capture a node from which the attacker can steal the key material [13].

1- Sybil attack

The attacking node is forged and it can disguise the identity of more than one node inside the network, thereby affecting data authenticity, confidentiality and data integrity [14].

2- Sinkhole attack

In general, malicious node disguises the victim nodes and is located near to the *BS* and persuades the victim nodes to send their messages to the BS at high power. Additionally, it may be likened to a black hole absorbing everything passing into it [13].

3- Wormhole attack

The malicious node uses a tunneling technique to establish itself between nodes in order to confuse the routing protocol. The malicious node disguises the victim nodes and shows itself as having higher communication resources than normal nodes in order to establish the best communication channels between them. Moreover, wrong routing of information leads to changes in the network topology and the stream of messages will change. It can alter the packet or modify it, thereby damaging the packet [13].

4- Hello flood attack

The intruder is a sink or *BS* and it broadcasts a hello message with strong transmission range and power to the network and acts as a fake sink to send their messages to it rather than to the legal sink. It disguises the BS by acting as a neighbor with many nodes in the

network, thereby badly mixing the network routing [13].

Proposed Scheme

A WSN consists of a large number of small, self-powered, and inexpensive devices that have ability to sense, compute, and communicate with each other through wireless techniques. Sensor nodes collect the sensing data from the environment then send collected data to the end user. Accordingly, the proposed scheme consists of the following:

1. The Network Model

The proposed method considered the heterogeneous structure for the network. The network consists of three levels: the top level comprises the *BS* with unlimited resources; the middle level consists of *CH* sensor which are high sensors working as *CH* with properties higher and operating with far more power than Low (*L)* sensors, which are also the sensors, but working at the last level of a network. Moreover, the routing of gathered information in the proposed network is central and prepared in a secure way by using the techniques of cryptography from the *L* sensors to the *BS* via the *CH* sensors. The latter works like a gateway. Furthermore, *L* sensors can be connected to the *CH* sensors directly or through other *L* sensors.

2. Assumption

The *BS* is trusted with a large memory size, high power processing, powerful transmission range, and unlimited battery energy.

a) The deployment area is 50 * 50 m^2.

b) Number of *CH* sensor is one and the numbers of L sensors are 100.

c) The *CH* has the ability for accessing to each *L* and not verse versa.

d) The range of all *L* sensors nodes transmission range is 15 meters.

e) After distribution (deployment) all sensors nodes (*CH* and *L*) are static and equipped with GPS (Global Positioning System).

f) *L* sensors and *CH* sensor equipped with tamper resistance which consider as a compromised immune system [15], where the algorithms store in it.

3. The Network Phases

The proposed scheme consists of three phases as depicted bellow:

a- Pre-distribution phase

The *CH* and *L*s are preloaded with algorithm 1 and 2. Besides, the spatial information of the *BS* is stored in the *CH* memory, and the latter uses it as a key to communicate to *BS*.

b- Distribution phase

Due to the random distribute of the sensors, the network topology is unpredictable. The BS is setup in a safe area near deployment area but in controlled area to observe the uncontrolled area.

Both of 100 *L* sensors and one *CH* scatter within 50*50 m^2 randomly in uncontrolled area. In addition, *L* sensors and *CH* are fixied after deployment and each *L* and *CH* uses their location as a key to communicate to each other.

c- Cluster forming phase

The clustering mechanisms used to enlarge the life-time of WSN and to provide more efficient functioning procedures makes the algorithm economical than the flat sensor network [16]. The cluster formation starts from the CH sensors and performs the following step:

1. After the deployment, To determine the absolute node positions in a relatively calibrated flat 2D net via GPS technique based on stored maps, landmarks [17]. The *BS* computes its location (X-axis and Y-axis) via GPS. Then, broadcast it to the *CH* by *equ.1* and algorithm 1. Where, the *BS* converts $(x-axis_{BS})$ to $(char_{x-axis-BS})$ and $(y-axis_{BS})$ to $(char_{y-axis-BS})$ for making the message secure. Because, the coordination of the sensors are often represented as float number. The output of the SHA-1dosen't contains the float number. If we make a concatenation between the coordination values (*x*,*y*) with the output of SHA-1, then it will be very easy for the hacker to estimate the exact values of (*x*,*y*). Therefore, their values are converted to sequence of characters. This will be embedded with the output of SHA-1 in MAC and never understoodable. Because the output not repeated except who has the algorithm can get it.

2. The *CH* sensor decrypts the received message according algorithm2. Then, extract s the location of the *BS*.

3. The *CH* sensor encrypts its location to stream of bits then broadcasts it to all nodes according *equ.2* and algorithm 1.

4. Each *L* decrypts the received message according algorithm 2. Then, extracts the location of the *CH*; Each *L* sensor calculates the distance by Euclidean mechanism according to *equ.3*.

In the end, each neighbor *L* sensor (L_{near}) which has distance less than 15 m can communicate directly with *CH* as *equ.4* and algorithm 1.

5. The *CH* sensor decrypts the received message according algorithm2. Then, it extracts the location of the (L_{near}). Later, the *CH* sensor sends the ACK (location of *L)* according to *equ.5* and algorithm 1.

6. Each (L_{near}) which is able to connect directly with the *CH* can decrypts the message and it makes the ACK true.

7. Each remote *L* sensor which doesn't receives the ACK because it is a long distance from the selected *CH* sensor (more than 15 m) sends a hello message to other L sensors according to *equ.6* and algorithm 1.

8. Each neighbor *L* (L_{near}) receives the messages within its coverage, and before decrypting the message, it checks whether, if it has the ACK or not. If it has the ACK then it decrypts the message according algorithm 2; otherwise, it discards the message.

9. The L_{near} sensors send the ACK according to *equ.7*. execution.

10. Each L_{remote} which is able to connect directly with the L_{near} can decrypts the message and it makes the

ISSN: 1813 – 1662 (Print)
E-ISSN: 2415 – 1726 (On Line)

ACK true. Moreover, the steps 8 and 9 repeat till all nodes conn-ects to each other as shown in figure 2, where it shows the number of simulation implementation.
.

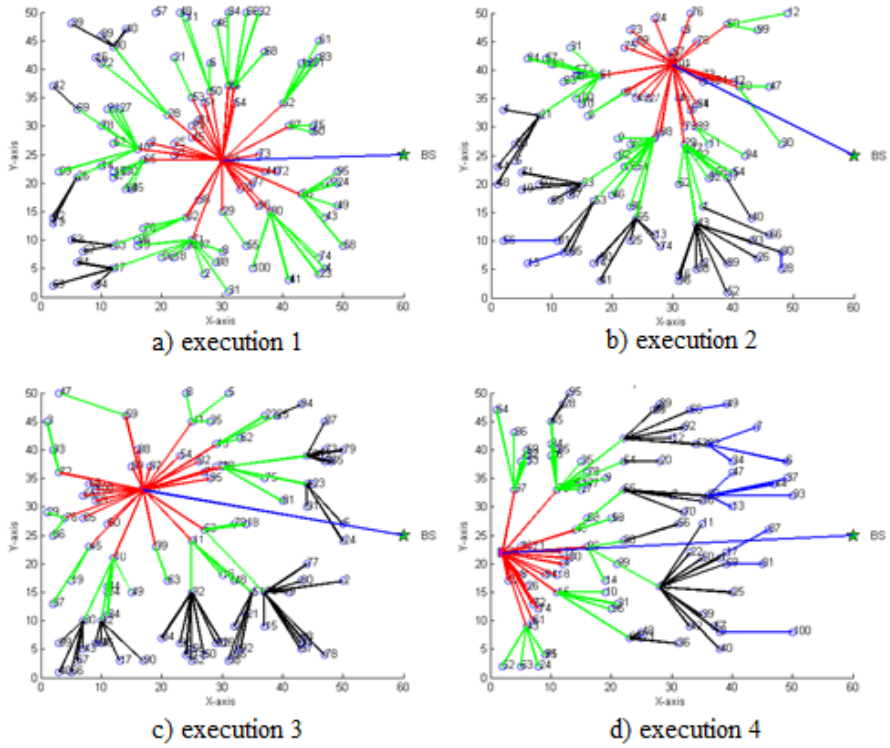

Figure 2 Network construction

$$BS \rightarrow CH : H(x-axis_{BS}) \parallel char_{x-axis-BS} \parallel' L' \parallel H(y-axis_{BS}) \parallel char_{y-axis-BS} \quad equ.1$$

$$CH \rightarrow L : H(x-axis_{CH}+w) \parallel char_{x-axis-CH} \parallel' L' \parallel H(y-axis_{CH}+w) \parallel char_{y-axis-CH} \quad equ.2$$

$$Distance = \sqrt[2]{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad equ.3$$

$$L_{near} \rightarrow CH : H(x-axis_{Lnear}+w) \parallel char_{x-axis-Lnear} \parallel' L' \parallel H(y-axis_{Lnear}+w) \parallel char_{y-axis-Lnear} \quad equ.4$$

$$CH \rightarrow L_{near} : H(x-axis_{Lnear}+w)\, char_{x-axis-Lnear} \parallel L' \parallel H(y-axis_{Lnear}+w) \parallel char_{y-axis-Lnear} \quad equ.5$$

$$L_{remote} \rightarrow L_{near} : H(x-axis_{Lremote}+w) \parallel char_{x-axis-Lremote} \parallel' L' \parallel H(y-axis_{Lremote}+w) \parallel char_{y-axis-Lremote} \quad equ.6$$

$$L_{remote} \rightarrow L_{near} : H(x-axis_{Lremote}+w) \parallel char_{x-axis-Lremote} \parallel' L' \parallel H(y-axis_{Lremote}+w) \parallel char_{y-axis-Lremote} \quad equ.7$$

Where (*H)* is SHA-1 , (||) is concatenation, (L) is a character and (*w)* is integer

Algorithm 1: Encryption the messages

1- Read real *x= x-axis*
2- Read real *y=y-axis*
3- Define *i,w* as integer
4- *w=1;*
5- Define p^1 , p^2 ,*has1, has2, M* as string
6- x^1=num2str(*x*);
7- y^1=num2str(*y*);
8- for *i*=1 To length (x^1)
  8-1- begin
  8-2- set_char{a,b,c,d,e,f,g,h,k,n,m}
  8-3- $p^1(i)$=index_of_set_char{i}
  8-4- *end*
9- for *i*=1 To length (y^1)
  9-1- begin
  9-2- set_char{a,b,c,d,e,f,g,h,k,l,n,m}
  9-3- $p^2(i)$=index_of_set_char{i}
  9-4- end
10- *has1* = *hash*((*x*+*w*),'SHA-1'); where SHA-1 is (Secure Hashing Algorithm 1)
11- *has2* = *hash*((*y*+*w*),'SHA-1');
12- *M* = [*has1*||p^1||*'L'*||*has2*||p^2];
  //where *M* is the encrypted message ready to send and '||' is a concatenation
13- Increment *w* ;
14- end

Algorithm 2: Decryption the messages

1- Define *j,i,w,* x^{new}, y^{new} as integer
2- Define *M, K,* b^1, b^2, a^1, a^2, p^3, p^4, p^4, p^4 , *Verifyhas1, Verifyhas2* as string
3- *w=0;*
4- *j*=length(*M*);
5- *K* = find(*M*=='L');

ISSN: 1813 – 1662 (Print)
E-ISSN: 2415 – 1726 (On Line)

6- b^1 = M(1:40);
7- b^2= M(41:K-1);
8- a^1=M(K+1:K+40);
9- a^2=M(K+41 To end);
//Extract the x-axis & y-axis
10- for i=1 To length (b^2)
10-1- begin
10-2- set_char{a,b,c,d,e,f,g,h,k,l,n,m}
10-3- $p^3(i)$=index_of_set_char{i}
10-4- end
11- for i=1 To length (a^2)
11-1- begin
11-2- set_char{0,1,2,3,4,5,6,7,8,9,.}
11-3- $p^4(i)$=index_of_set_char{i}
11-4- end
12- x^{new}=str2num(x);
13- y^{new}=str2num(x);
14- *Check w value of sender*
15- Increment *w;*
16-*Verifyhas1 = hash*((x^{new}+*w*),'SHA-1');
17-*Verifyhas2 = hash*((y^{new}+*w*),'SHA-1');
18-if (*Verifyhas1* == b^1
& *Verifyhas2* == a^1)
18-1- Save *x-axis*
18-2- Save *y-axis*
19- else
19-1- Discard *M*
20- end

In addition, to understand the **algorithm 1**, assume the location of L_1 (X,Y) = (25.34, 34.42) need to encrypt; it will be encrypted as following:

1. X= (25.34) converts to (cfmde). Steps 8,8-1,8-2,8-3,8-4.
2. Y= (34.42) converts to (demec). Steps 9,9-1,9-2,9-3,9-4.
3. *has1*=963987858667d2be96c8ee2612bf67ae15f1cf06. Step 10.
4. *has2*=9e7697657a35126bd9719f0cff06cfc3d5ef36cc. step 11.
5. *M*=963987858667d2be96c8ee2612bf67ae15f1cf06cfmdeL9e7697657a35126bd9719f0cff06cfc3d5ef36ccdemec. step 12.
6. *w=2;* step 13.

Moreover, the decryption of the message M done by the **algorithm 2** as the following:

1. *M*=963987858667d2be96c8ee2612bf67ae15f1cf06cfmdeL9e7697657a35126bd9719f0cff06cfc3d5ef36ccdemec.
2. b^1=963987858667d2be96c8ee2612bf67ae15f1cf06. Step 6.
3. $b^{2=}$cfmde. Step 7.
4. a^1=9e7697657a35126bd9719f0cff06cfc3d5ef36cc. step 8.
5. a^2= demec. Step 9.
6. P^3= 25.34.steps 10,10-1,10-2,10-3,10-4.
7. P^4= 34.42. steps 11,11-1,11-2,11-3,11-4.
8. x^{new}=25.34.step 12.
9. y^{new}=34.42.step 13.
10. *W=1;* step 15
11. *Verifyhas1=* 963987858667d2be96c8ee2612bf67ae15f1cf06. Step 16.
12. *Verifyhas2=* 9e7697657a35126bd9719f0cff06cfc3d5ef36cc. Step 17.
13. (*Verifyhas1=*b^1 &*Verifyhas2=*a^1).Step18.
14. 25.34 Save as *x-axis.* Step 18-1.
15. 34.42 Save as *y-axis.* Step 18-2.

Security goals analysis:

The security goals analysis is the main part in our proposed scheme as given below:

1) **Authentication**: This is achieved because each node has a unique key (location), as well as the use of HMAC in the deployment phase which acts as a one way function.

2) **Confidentiality**: The proposed scheme encrypts every message and makes it secrets by mean of the proposed algorithms using HMAC. In traditional Hash when Alice sends a message to Bob, initially she must send two messages (the digest and the plain text). This leads to make confidentiality failed. Also, same thing when utilizes traditional MAC. But, in the proposed method one encrypted message is sent rather than two.

3) **Integrity**: The proposed scheme protects the received messages from alteration and modification it by using HMAC in the proposed algorithms.

4) **Scalability**: the proposed scheme is wor-king properly around 200 nodes. This is approved by simulating, as shown in figure 3 where the node (6) not connected.

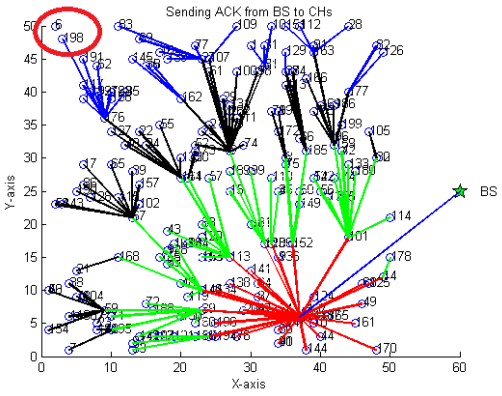

Figure 3 Comparison in term of connectivity

5)**Connectivity**: in the proposed scheme all nodes communicates to each other for creating the network, as shown in adapted Figure 4. Moreover, hops numbers in the proposed scheme are lower than the compared scheme [18, 19] as shown in adopted figure 3 and the connectivity rate in the proposed scheme is 100%;but, in [19] is not 100%.

In addition, if comparing the proposed scheme with [9, 18, 19] in term of number of hops, the proposed scheme's hops are less than other schemes as shown in figure 4 and table 1.

Also, when matching the proposed scheme with [9] in number of *CH* the last uses **two** *CH*; but, the proposed scheme uses **one** *CH* as shown in figure 4

ISSN: 1813 – 1662 (Print)
E-ISSN: 2415 – 1726 (On Line)

which leads to reduce the cost**.** As well as, number of hops in [9] are **five**; but, the proposed scheme are **four**. Because that the proposed scheme better than [9, 18, 19] in term of energy consumption.

Furthermore, we compare the proposed scheme with some existing schemes in term of security analysis as shown in table 2.

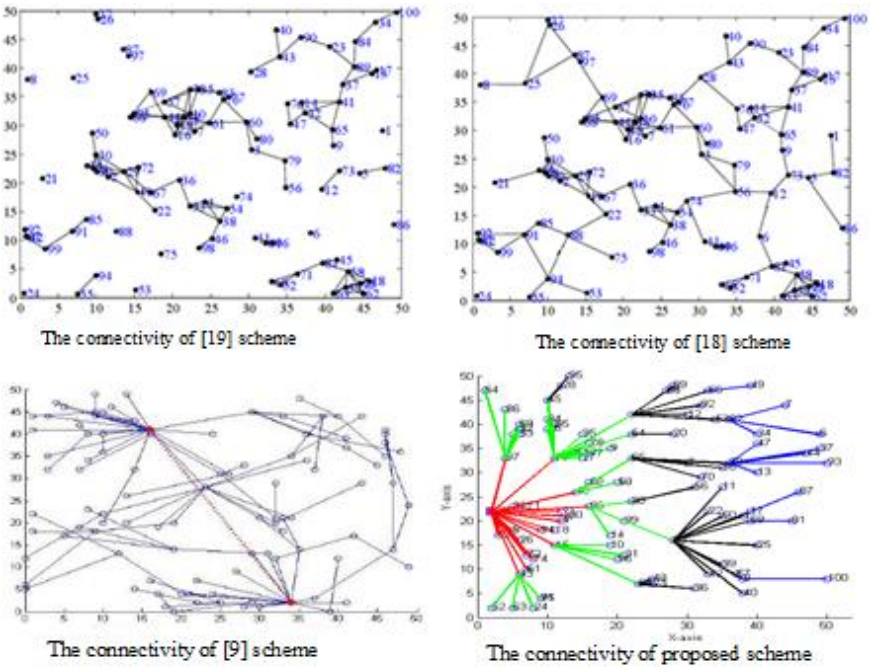

Figure 4 Comparison in term of connectivity

Table 1 Comparison the proposed scheme with 9,18,19 schemes

Requirements	Proposed scheme	Scheme[9]	Scheme[18]	Scheme[19]
Connectivity	**100%**	**100%**	**100%**	**87%**
No. of cluster	**1**	**2**	**1**	**4**
No. of hops	**4**	**5**	**10**	**16**

Table 2 Comparison in term of security

Requirements	Proposed scheme	Scheme[20]	Scheme[21]	Scheme[22]
Authentication	One-way	One-way	One-way	One-way
Confidentiality	Satisfies	Does not Satisfies	Does not Satisfies	Does not Satisfies
Integrity	Satisfies	Does not Satisfies	Does not Satisfies	Does not Satisfies
Scalability	Satisfies	Satisfies	Satisfies	Satisfies
Cryptographic mecha-nism	Hash function and MAC	PKI based on ECC	Self-certified key	Hash function and XOR

Attacks analysis:

The proposed scheme is effective versus the follow-ing attacks:

1. Eavesdrops attack gets the signal. It does not con-clude what is inside the message because the message content is a stream bit of characters and numbers without original pla-intext. The message was en-crypted since it does not know the encryption algo-rithm to extract the original message. The proposed scheme is resistance to this attack because the loca-tion converted sequence of charact-er. Then embed-ded with the output of SHA-1 in MAC according to proposed algorithms which make the output never understood able because it never repeated.
2. Sybil attack tries to transmit a message to legiti-mate nodes within the network with a fake *ID*. But, the proposed scheme based on spatial location rather than *ID*. Therefore, it cannot affect the network. Fur-thermore, the message not contains the plaintext. Be-cause that the attacker cannot gain the key.

3. The proposed scheme rejects the sinkhole attack messages because only the *CH* sensors can communicate with the *BS*. Furthermore, in pre-distribution the spatial location of *BS* saved in CH, which uses to exchange the messages, where the attacker cannot know the spatial location of *BS* and the algorithms. Because that the attacker message will be discarded.
4. Hello flood attack cannot affect the proposed scheme because it uses a hello message with spatial location converted to data sequence then encrypted by HMAC. The attacker message can be recognized from the nodes within the network. Therefore, it will be rejected.
5. Wormhole attacks want to occur between two legal nodes and exchange fake massages with each legal node. Each *CH* and *L* can detect this attack because it uses HMAC to verify the message and discard any malicious node messages.

In addition, we compare the proposed scheme with some existing schemes [23] in term of attacks as shown in table (3).

Table 3 Comparison in Terms of attack

Scheme / Attack	Scheme [24]	Scheme [25]	Proposed scheme
Eavesdropping	Does not Satisfies	Does not Satisfies	Satisfies
Hello flood	Does not Satisfies	Satisfies	Satisfies
Worm-hole	Satisfies	Satisfies	Satisfies
Sink hole	Satisfies	Satisfies	Satisfies
Sybil	Satisfies	Does not Satisfies	Satisfies

In addition, the table 4 and figure 5 mention the *L* sensor time consuming measured in second, display time consuming in each *L* sensor for encryption/decryption when it simulating via MATLAB R2013a for Mica2 with processor 433 MHz and memory 128K bytes.

Table 4 Time consuming measure in second

Operation in each L	Time in second
Encryption	0.882499
Decryption	0.484585
1st hop	1.367085
2nd hop	4.133530
3rd hop	5.500600
4th hop	6.867670

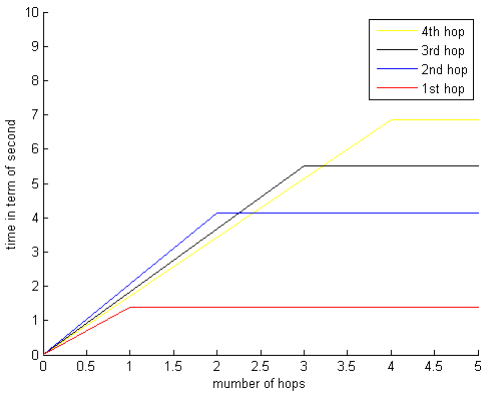

Figure 5 time consuming in hops

Finally, the figure 6 shows the time consuming measured in second for each L in one round.

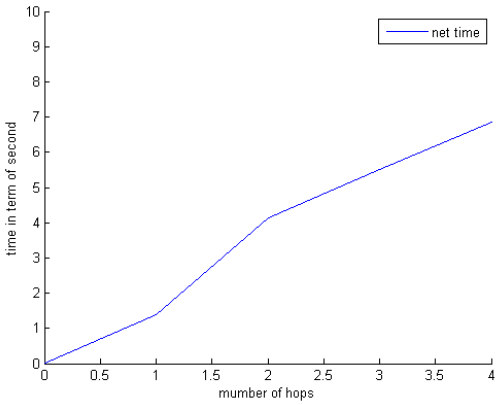

Figure 6 Time consuming in one round

Conclusion

In a manner corresponding to the assessments metric in all previous papers in the field of security and key management for WSN, including the proposed scheme, it finds that all the key management schemes had cons encompasses the trade-off between network the security analysis, the attacks and energy consumption, time, scalability and connectivity. Hence, providing the ideal key management scheme which can cover all the challenges are still valuation searching area and difficult work.

The proposed scheme focused on heterogeneous routing in WSNs over the use of a new enhanced reactive scheme, which aims at the achievement of power cluster forming due to decrease the number of hops in the routing, security analysis, scalability, connectivity and attacks in the WSN based on spatial location, which is used as a key to make secure link between the nodes in the network.

Reference

[1] K. Rasul, N. Nuerie, and A. S. K. Pathan, *2010,*"An Enhanced Tree-Based Key anagement Scheme for Secure Communication in Wireless Sensor Network," in *High Performance Compu-ting and Communications (HPCC), 12th IEEE International Conference* , pp. 671-676.

[2] Y. Zhang and J. Pengfei, 2014, "An efficient and hybrid key management for heterogeneous wireless sensor networks," in *The 26th Chinese Control and Decision Conference (CCDC),* pp. 1881-1885.

[3] A. Tajeddine, A. Kayssi, A. Chehab, and I. Elhajj, 2014, "Authentication schemes for wire-less sensor networks," in *MELECON 17th IEEE Mediterranean Electrotechnical Conference*, pp. 367-372.

[4] F. Legendre, G. Dequen, and M. Krajecki, 2012, "Encoding Hash Functions as a SAT Prob-lem," in *IEEE 24th International Conference on Tools with Artificial Intelligence*, pp. 916-921.

[5] A. A. Alkandari, I. F. T. Alshaikhli, and M. A. Alahmad, 2013, "Cryptographic hash function: A high level view,",*IEEE International Conference on Informatics and Creative Multimedia*, PP. 128-134.

[6] M. I. Salam, P. Kumar, and L. HoonJae, 2010, "An efficient key pre-distribution scheme for wireless sensor network using public key cryptography," in *Networked Computing and A-dvanced Information Management (NCM), Sixth International Conference on*, pp. 402-407.

[7] R. K. Kodali, 2014, "Key management technique for WSNs," in *Region 10 Symposium, IEEE*, pp. 540-545.

[8] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, 2000, "Energy-efficient communication protocol for wireless microsensor networks," in *System Sciences, Proceedings of the 33rd Annual Hawaii International Conference on*, p. 10 pp. vol.2.

[9] A. C. Shakir, J. Min, and G. Xuemai, 2012, "Elliptic Curve Cryptography Based Scheme for Key Predistribution in the Heterogeneous Wirel-ess Sensor Network," *wulfenia*, vol. 19, pp. 131-142.

[10] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, 2006, "Recommendation for key management-part 1: General (revised," in *NIST sp-ecial publication*.

[11] R. Yasmin, 2012, "An efficient authenticat-ion framework for wireless sensor networks," Ph.D, thesis, University of Birmingham.

[12] T. Lalitha and A. J. Devi, 2014, "Security in Wireless Sensor Networks: Key Management Module in EECBKM," in *Computing and Commu-nication Technologies (WCCCT), World Congress on*, pp. 306-308.

[13] G. Gulhane and N. V. Mahajan, 2014, "Securing Multipath Routing Protocol Using Authentication Approach for Wireless Sensor Networ-k," in *Communication Systems and Network Tec-hnologies (CSNT), Fourth International Confere-nce on*, pp. 729-733.

[14] P. R. Vamsi and K. Kant, 2014, "A light-weight Sybil attack detection framework for Wi-reless Sensor Networks," in *Contemporary Com-puting (IC3), Seventh International Conference on*, pp. 387-393.

[15] Q. Yang, Q. Li, and S. Li, 2008, "An Efficient Key Management Scheme for Heterogeneous Sensor Networks," in *4th International Confere-nce on Wireless Communications, Networking and Mobile Computing*, pp. 1-4.

[16] L. M. C. Arboleda and N. Nasser, 2006, "Comparison of Clustering Algorithms and Protoco-ls for Wireless Sensor Networks," in *Canadian Conference on Electrical and Computer Enginee-ring*, pp. 1787-1792.

[17] N. Bulusu, J. Heidemann, D. Estrin, and T. Tran, 2004,"Self-configuring localization system-s: Design and experimental evaluation," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, pp. 24-60.

[18] K. Rajendiran, R. Sankararajan, and R. Palaniappan, 2011, "A secure key predistribution sc-heme for WSN using elliptic curve cryptogr-aphy," *ETRI Journal*, vol. 33, pp. 791-801.

[19] R. Blom, 1984, "An optimal class of symm-etric key generation systems," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 335-338.

[20] Z. Benenson, F. C. Gärtner, and D. Kesdog-an, 2004, "User Authentication in Sensor Netw-orks," in *GI Jahrestagung (2)*, pp. 385-389.

[21] C. Jiang, B. Li, and H. Xu, *2007,* "An efficie-nt scheme for user authentication in wireless sensor networks," in *Advanced Information Net-working and Applications Workshops, AINAW-'07. 21st International Conference on*, pp. 438-442.

[22] H.-R. Tseng, R.-H. Jan, and W. Yang, 2007, "An improved dynamic user authentication sch-eme for wireless sensor networks," in *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, pp. 986-990.

[23] Y. Zhang, X. Li, J. Liu, J. Yang, and B. Cui, 2012, "A secure hierarchical key management scheme in wireless sensor network," *Internat-ional Journal of Distributed Sensor Networks*,PP. 1-8.

[24] S. Hussain, F. Kausar, and A. Masood, 2007, "An efficient key distribution scheme for heterogeneous sensor networks," in *Proceed-ings of the international conference on Wireless communications and mobile computing*, pp. 388-392.

[25] B. Maala, H. Bettahar, and A. Bouabdallah, 2008, "TLA: A Tow Level Architecture for Key Management in Wireless Sensor Networks," in *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*, pp. 639-644.

Tikrit Journal of Pure Science 22 (6) 2017 *ISSN: 1813 – 1662 (Print)*
E-ISSN: 2415 – 1726 (On Line)

تشكيل المجموعات بالاعتماد على المعلومات المكانية باستعمال HMAC في شبكات الحساسات اللاسلكية

اسو احمد مجيد

فرع صحة عامة بيطرية ، كلية الطب البيطري ، جامعة كركوك ، كركوك ، كركوك ، العراق

الملخص

يعتبر اجهزة استشعار اللاسلكية واحدة من أكثر التكنولوجيات الرئيسية من خلال استخدامه في التطبيقات المختلفة مثل التطبيقات البيئية، والتطبيقات العسكرية والتطبيقات التجارية وتطبيقات الصحة والتطبيقات الزراعية. ونظرا لنشر وتوزيع هذه الشبكات في المناطق المفتوحة (منطقة غير مسيطرة عليه)، وخاصة في التطبيقات العسكرية، في مثل هذه الحالات تكون العقد معرضة للالتقاط من قبل العدو. بالإضافة إلى ذلك، قد يتم مراقبة واعتراض حزم البيانات أو تعديلها نظرا لطبيعة الارسال. ونتيجة لذلك، الأمنية الأجهزة مثل التوثيق والتشفير يتم القيام به من قبل إدارة المفاتيح وهي ليست بالأمر الهين. إدارة المفاتيح مهمة للحفاظ وادامة عمليات الشبكة. المخطط المقترح فيها العقد تعتمد على المعلومات المكانية مع استخدام متسلسلة ليرسل رسائل مشفرة لبعضها البعض بطريقة آمنة عن طريق HMAC وتوفير وصلات آمنة بين العقد في الشبكة لتشكيل مجموعات.

الكلمات المفتاحية: شبكات الاستشعار اللاسلكية الغير المتجانسة، تشفير المفتاح المتماثل، SHA-1، MAC، الهجمات في شبكات الاستشعار اللاسلكية.