Qian Fang; Ying Liu; Xiaoqun Zhao
A chaos-based secure cluster protocol for wireless sensor networks

Kybernetika, Vol. 44 (2008), No. 4, 522--533

Persistent URL: http://dml.cz/dmlcz/135871

KYBERNETIKA — VOLUME 44 (2008), NUMBER 4, PAGES 522 – 533

A CHAOS–BASED SECURE CLUSTER PROTOCOL FOR WIRELESS SENSOR NETWORKS

Qian Fang, Ying Liu and Xiaoqun Zhao

Security mechanisms for wireless sensor networks (WSN) face a great challenge due to the restriction of their small sizes and limited energy. Hence, many protocols for WSN are not designed with the consideration of security. Chaotic cryptosystems have the advantages of high security and little cost of time and space, so this paper proposes a secure cluster routing protocol based on chaotic encryption as well as a conventional symmetric encryption scheme. First, a principal-subordinate chaotic function called N-Logistic-tent is proposed. Data range is thus enlarged as compared to the basic Logistic map and the security is enhanced. In addition, the computation is easier, which does not take much resource. Then, a secure protocol is designed based on it. Most of communication data are encrypted by chaotic keys except the initialization by the base station. Analysis shows that the security of the protocol is improved with a low cost, and it has a balance between resource and security.

Keywords: wireless sensor network, security, chaotic encryption, cluster

AMS Subject Classification: 90B18, 74H65, 68M12

1. INTRODUCTION

Wireless sensor networks (WSN) are appealing to researchers due to their wide range of potential applications in military, industry, home networks, and so on. However, since WSN suffer from many constraints including small memory, restricted computing capability, dynamic topology and limited energy, the security mechanisms for traditional networks canot be directly applied to WSN, so a number of open problems and challenges remain [8], and secure protocol is one of them.

Most of routing protocols for WSN are not designed in consideration of security. Recently, some security optimization for routing have been proposed. Since WSN suffer from limited resources, asymmetric cryptosystem which consumes more resources is not suitable for WSN, so symmetric encryption is commonly used in secure protocols. SPINS [6] is a suitable secure protocols for WSN. Many research approaches afterwards adopt the ideas one way or another. However, SNEP, which is one part of SPIN, assumes that each sensor is given a key shared with the base station (BS) and other keys are all derived from it, so it is totally dependent on BS.

Also, it does not give any detail of key distribution. What's more, SPINS is not fully specified.

Chaos is a kind of complex, nonlinear, non-balanced dynamic process in mathematics and physics. The features of chaos system such as sensitivity to initial values, inscrutability, and so on, make it adaptable to encryption. Chaotic cryptosystem is an emerging encryption technology. It has the advantages of high security and low cost of time and space, and chaos-based security communication systems have been widely studied recently [2]. However, chaos-based WSN security protocol has not been carefully studied. This paper proposes a secure cluster protocol based on chaotic encryption as well as a conventional symmetric encryption scheme.

2. CHAOS–BASED ENCRYPTION

A chaos-based cryptosystem uses a chaotic system as the key generator. A chaotic sequence is generated based on an initial value, and the sequence, used as a key, is added to the plaintext. Then, the ciphertext is generated. The same chaotic sequence is used for decryption [10]. In a chaos-based cryptosystem, the sender and the receiver need exactly the same chaotic sequence. Even if there is only very little difference between the two initial values, the sequence will be much different after some time. So chaos synchronization is crucial. Because the chaotic signal is non-periodic, near-random, sensitive to initial values, complex in dynamic characteristics, and its distribution is not coincident to statistics, the forecast and reconstruction of the chaotic signal are very difficult. The chaos-based cryptosystem is preponderated over the conventional cryptosystem [1]. It is suitable for wireless networks with limited resources due to its high security and low cost of time and space [7].

2.1. The logistic map

WSN usually has very limited resources, so the algorithm should be as simple as possible. Recently a chaotic Logistic map is used as a one-dimensional discrete chaotic system [4]. The Logistic equation is

$$x_{n+1} = \lambda x_n(1 - x_n), \quad x \in (0,\ 1), \quad \lambda \in [0,\ 4] \tag{1}$$

When $\lambda \geq 3.5699$, the sequence generated by this map will be chaotic. Another Logistic map is $x_{n+1} = 1 - \lambda x_n^2$, $x \in (-1, 1)$, $\lambda \in [0, 2]$.

Logistic map has good chaotic characteristics. The probability distribution function is independent of initial values, the system is ergodic, the statistical average of sequences of the above two chaotic maps are respectively 0.5 and 0, the autocorrelation is close to a δ function, and the correlation of any two sequences generated by two different initial values or λ is 0. Therefore, a chaotic sequence is close to white noise, and is appropriate for encryption. This chaotic system is easy to implement, and there is no need for complex computation, so it is suitable for sensor nodes.

However, the basic Logistic map is a continuous function in (0, 1), while WSN is a kind of digital communication system. No matter what digital system and computer are used, the corresponding function is not continuous, and x_i and λ have

only limited points to be used in the range of (0, 1). So the function is not a truly chaotic one, because ergodicity will not be held in the whole interval (0, 1). Suppose the number of x_i is i_{xi} and the number of λ is j_λ in its range. Then, the data space can be denoted as an array $[i_{xi}, j_\lambda]$. The data range of x_i and λ is relatively small, so the number of elements in the array is also relatively small, thus breaking is comparably easy. So, in order to increase the security, the digital chaotic function should be closer to have ergodicity. The larger the data range of x_i and λ are, the more secure the system becomes.

Logistic map is a one-parameter and one-dimensional chaotic function, and the range of the sequence values as well as of the parameter are relatively small, so its security is relatively low. This paper proposes a new scheme with a low digital computational cost and a wider data range, as further discussed below.

2.2. N-logistic-tent map

(1) In order to enlarge the data range of x_i, this paper modifies the Logistic map as

$$x_{n+1} = \mu x_n(N - x_n/m)/N, \quad x \in (0, mN), \quad \mu \in (0, 4) \tag{2}$$

where $N = 2^K$, $m = 2^k$, K and k are both integers. When $\mu \geq 3.5699$, the sequence

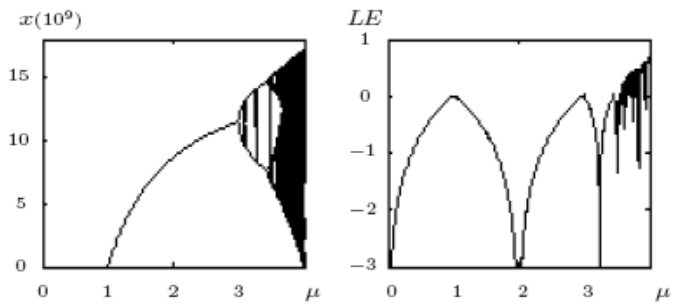

Fig. 1. (a) period-doubling bifurcation. (b) Lyapunov exponent.

generated by this map will be chaotic. Since m and N are powers of 2, the process in the microcontroller has binary operations, and the output is also binary. And it only needs addition, multiplication and shift operations, so it will not take much computing resource. Of course, only when $mN \to \infty$, the sequence is ergodic, so the larger the mN is, the better the chaotic sequence performs. The value depends on the need of the output precision as well as the computational ability and the memory of the microcontroller. For example, $K = 32$, $N = 2^{32} = 4294967296$, where N corresponds to four bytes in the wireless microcontroller chip.

To show that equation (2) has good chaotic features, a proof of its self-mapped property is first given as follows: When $0 < x_n < mN$, x_{n+1} can be considered as μm times the area of a rectangle, the two sides of which are $(\frac{x_n}{m})$ and $(N - \frac{x_n}{m})$. The sum of the two sides is a certain value N, so when the rectangle is a square, the area is the largest, which is $\frac{N^2}{4}$, therefore $(\frac{x_n}{m})(N - \frac{x_n}{m})$ belongs to $[\,0, \frac{N^2}{4}]$. Substituting it into equation (2), so $x_{n+1} \in (0, mN)$, i. e., the self-map feature is proved.

The chaotic function to be the self-mapped shows that the value of x_{n+1} is bounded. And after that one can compute the Lyapunov exponent (LE), which can be used to judge whether the sequence is a chaotic one [3, 5].

$$\mathrm{LE} = \frac{1}{J}\sum_{i=1}^{J} \ln\left|\frac{\mathrm{d}x_{i+1}}{\mathrm{d}x_i}\right| = \frac{1}{J}\sum_{i=1}^{J} \ln\left|\frac{x_{i+1}(x_i+\delta)-x_{i+1}(x_i)}{\delta}\right| \quad (J\to\infty) \qquad (3)$$

where $\frac{\mathrm{d}x_{i+1}}{\mathrm{d}x_i}=\frac{x_{i+1}(x_i+\delta)-x_{i+1}(x_i)}{\delta}$. The period-doubling bifurcation curve and the Lyapunov exponent curve are simulated when $K = 32$, $N = 2^{32} = 4294967296$. Figure 1 (a) shows the period-doubling bifurcation curve of the N-logistic map, which is similar to the basic Logistic map, but the range of sequence values is enlarged by mN times. Figure 1 (b) shows the LE curve, when $\mu \geq 3.5699$, LE> 0, so the N-Logistic map performs chaotic all. And the chaotic behavior can also be proved from the four bifurcations in Figure 1 (a). The computing process takes advantage of 2 to the Kth power, so digital division can be completed by shift operations. It is easy and suitable for WSN. Moreover, the value range of x is much enlarged, which will increase the size of the key space.

However, this is not enough. The range of $4 > \mu > 3.5699$ has not been enlarged and when $\mu > 3.5699$ there are also a few points with LE< 0. Moreover, the system is still one-parameter and one-dimensional, so the security is limited.

(2) Another chaotic map is introduced and the function is finally modified to an N-Logistic-tent map. The key value is modified from (x_i, λ) to (x_i, y_i, μ, β, m, N). The N-logistic map (4a) in the first step is used as the principal chaotic function and the N-tent map (4b), which is modified from the tent map, is used as the subordinate function. Tent map is denoted as $y_{n+1} = 1- \mid 1 - 2\, y_n \mid$, $y \in (0, 1)$ [3]. Suppose $\beta = 1 \sim 2$, $-y_n/2$ is added to the principal chaotic function (4a), and the two-dimensional N-logistic-tent map is proposed:

$$\begin{aligned} x_{n+1} &= \mu x_n(N - x_n/m)/N - y_n/2, \quad x \in (0, mN), \quad \mu \in (0, 4) && \text{(4a)} \\ y_{n+1} &= \beta(N - |N - y_n|), \quad y \in (0, 2N), \quad \beta \in [1, 2]. && \text{(4b)} \end{aligned}$$

The N-tent map (4b) enlarges the data range of the basic tent by $2N$, and the parameter β is also added. N-tent map (4b) is proved to be self-mapped. After that, the similar period-doubling bifurcation curve and the Lyapunov exponent curve prove that the N-tent map appears to be chaotic when $\beta = 1 \sim 2$.

In order to compute the Lyapunov exponent of the principle-subordinate chaotic function, a two-dimensional Lyapunov exponent is used as follows:

$$\begin{aligned} \mathrm{LE} &= \mathrm{LE}_x + \mathrm{LE}_y = \frac{1}{J}\sum_{i=1}^{J} \ln\left|\frac{\mathrm{d}x_{i+1}}{\mathrm{d}x_i} * \frac{\mathrm{d}y_{i+1}}{\mathrm{d}y_i}\right| \\ &= \frac{1}{J}\sum_{i=1}^{J} \ln\left|\frac{x_{i+1}(x_i+\delta)-x_{i+1}(x_i)}{\delta} * \frac{y_{i+1}(y_i+\delta)-y_{i+1}(y_i)}{\delta}\right| (J\to\infty) \qquad (5) \end{aligned}$$

where $\frac{\mathrm{d}x_{i+1}}{\mathrm{d}x_i}=\frac{x_{i+1}(x_i+\delta)-x_{i+1}(x_i)}{\delta}$, $\frac{\mathrm{d}y_{i+1}}{\mathrm{d}y_i}=\frac{y_{i+1}(y_i+\delta)-y_{i+1}(y_i)}{\delta}$. Taking $m = 4$, $K = 32$ and $N = 2^{32} = 4294967296$ as an example, the simulation result is shown in Figure 2

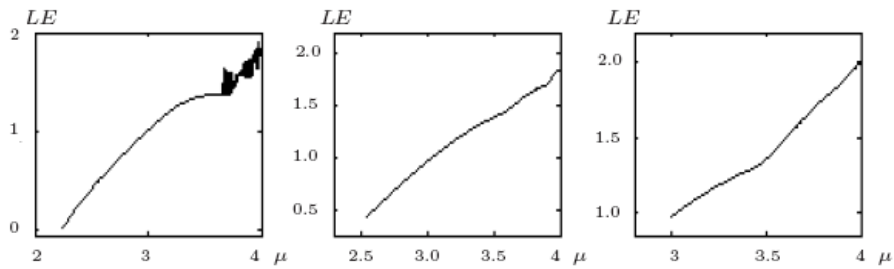

Fig. 2. (a) $\beta = 1.25$ (b) $\beta = 1.55$ (c) $\beta = 1.99$.

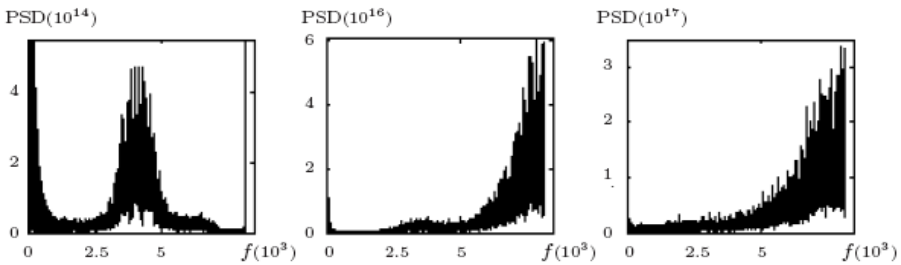

Fig. 3. (a) $\beta = 1.25$, $\mu = 2.25$ (b) $\beta = 1.55$, $\mu = 2.25$ (c) $\beta = 1.99$, $\mu = 3.0$.

to Figure 4. Figure 2 shows the Lyapunov exponent curve of the N-logistic-tent map when $\beta = 1.25$, $\beta = 1.55$, $\beta = 1.99$. The range of μ of LE > 0 is enlarged and the critical point $\mu_{\min}$ of μ when LE > 0 is related to β, expressing as $\mu_{\min} \approx 1 + \beta$ by simulation. One can also see from Figure 2 that the curve is discontinuous when $\mu = 2.25$ (LE $= 0.05$), $\mu = 2.55$ (LE $= 0.45$) and $\mu = 3.0$ (LE $= 0.95$). Figure 3 shows the power spectral density of the N-Logistic-tent for $\mu < 3.5699$, where the basic Logistic map does not appear to be chaotic. The parameters are $(\beta, \mu) = (1.25, 2.25)$, (1.55, 2.55) and (1.99, 3.0). The spectrum is a continuous one and appears a wide peak, which proves the map to be chaotic. And more spectrum computation shows that the power spectral density has no solution when $\mu < \mu_{\min}$, which means that the result is the same as the LE curve. Figure 4 shows three phase trajectories when $\beta = 1.5$ and $\mu = 3.99$, $\mu = 3.0$, $\mu = 2.5$, respectively. This trajectory portrait covers a whole area, which can also prove that the map is a chaotic one.

In the N-Logistic-tent map, first, the data range is enlarged, x is enlarged from $x \in (0, 1)$ to $x \in (0, mN)$, and y is added, so the whole data range is mN times the range of the basic Logistic map. Then, the digital chaotic function is closer to ergodicity, so the security is increased. Secondly, the parameter β is also added, and the value range of μ when the sequence is chaotic is also enlarged, which also increases the security. Last but not the least, the N-Logistic-tent map does not need complex computations. The code space by C language nearly take 1224 bytes, which is a little more than 1K bytes. This can be completed in a wireless microcontroller. So the N-Logistic-tent map increases the security with only a little higher complexity.

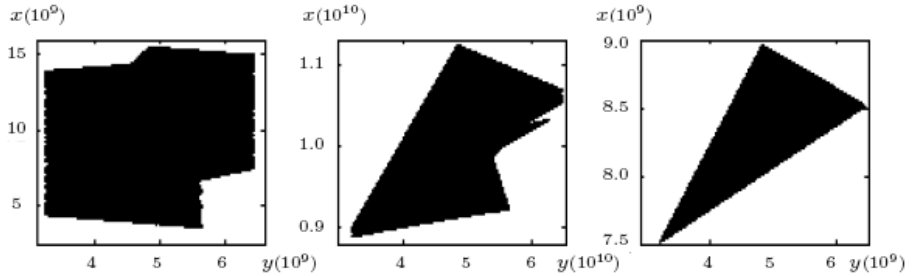

Fig. 4. (a) $\beta = 1.5$, $\mu = 3.99$ (b) $\beta = 1.5$, $\mu = 3.0$ (c) $\beta = 1.5$, $\mu = 2.5$.

Another equation of the N-logistic-tent map is expressed as $x_{n+1} = \mu x_n(N - x_n/m)/N^2 - y_n/2$, $x \in (0, mN)$, $\mu \in (0, 4N)$, $y_{n+1} = \beta x_n(N - |N - x_n|)/N$, $y \in (0, 2N)$, $\beta \in [N, 2N]$, in which x, y, μ, β are all integers.

2.3. Chaotic encryption based on the N-Logistic-tent map

Use $(x_i, y_i, \mu, \beta, m, N)$ as a seed key. Then, the chaotic sequences generated are used as encryption keys. When a data packet is sent, first of all a guide sequence like preamble is sent, which will be used for synchronization.

In encryption and decryption processes, data and chaotic sequences are computed together by some kind of rules. For WSN, simple ones should be used, such as the exclusive OR operation and ADD operation. The sequence after operation is ciphertext and sent to the next hop. The receiver decrypts it with the synchronous chaotic sequence and the same computational rules. A data set of 2^{25} *sinc* is taken as an example, the encryption and decryption processes of which is the same as digital data.

It can be seen from Figure 5 and Figure 6 that the data is renewable in encryption and decryption since the key $(x_i, y_i, \mu, \beta, m, N)$ is the same for sender and receiver, where Figure 5 (a) is the N-Logistic-tent chaotic waveform in encryption, Figure 5 (b) is the data waveform, Figure 5 (c) is the ciphertext waveform, Figure 6 (a) is the decryption chaotic waveform, Figure 6 (b) is the decrypted data_r waveform. In addition to the keys for encrypting plaintext, another segment of the sequence is needed for message authentication code. When the β of receiver is shorter by 2^{-52}, the decrypted data_r waveform looks like Figure 5 (c), in which the data_r is not renewable.

3. SECURE CLUSTER PROTOCOL FOR WSN BASED ON THE N-LOGISTIC-TENT CHAOTIC MAP FOR ENCRYPTION

3.1. Assumptions

(1) Network is partitioned into clusters.

(2) Cluster members can directly communicate with the cluster head.

(3) All nodes within a cluster maintain chaotic synchronization.

(4) The mobility of nodes is small.

(5) Each node shares an initial key with the base station.

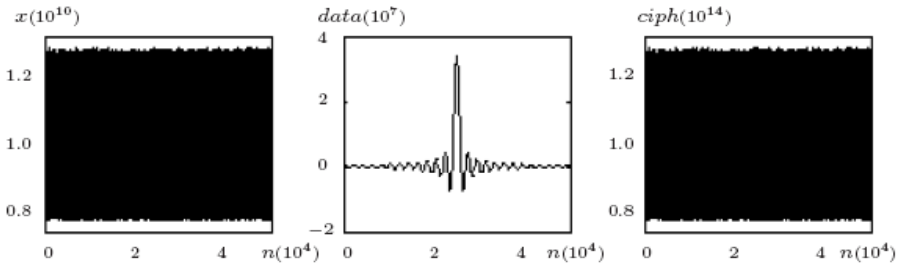

Fig. 5. (a) N-Logistic-tent (b) data (c) ciphertext.

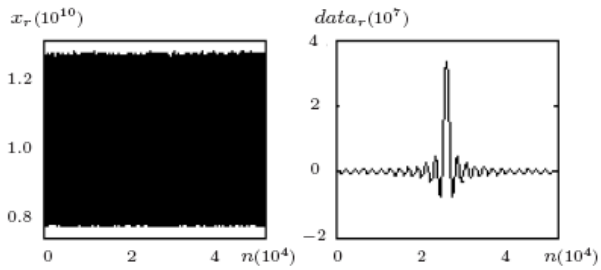

Fig. 6. (a) decryption chaotic (b) data$_r$.

3.2. Network architecture

Ad hoc and sensor networks are different from traditional networks. The proposed routing protocols can be divided into complanate routing and hierarchical routing according to the network architecture. Cluster-based protocol is a kind of energy-efficient hierarchical WSN protocol, in which the network is partitioned into clusters, as depicted in Figure 7, where a cluster has a cluster head and several cluster members, and several cluster heads can form a higher hierarchy cluster, till the highest sink node. In the cluster-based routing protocol, a cluster head not only collects and aggregates the information within its home cluster, but also forwards messages between clusters. Some popular clustered routing protocols are LEACH, PEGASIS, TEEN and so on [9]. They usually use TDMA or CDMA MAC mechanisms to decrease conflict among cluster members.

Cluster-based architecture partitions the whole network into many subnets, so all nodes within a cluster can share a synchronous chaotic system. All the messages transmitted in this cluster are encrypted with chaotic keys generated by this chaotic system. The receiver, which is usually a cluster head, decrypts by using the synchronous chaotic signals. Of course, there may also be some broadcast messages sent from the cluster head to cluster members. Traditional schemes often need two dif-

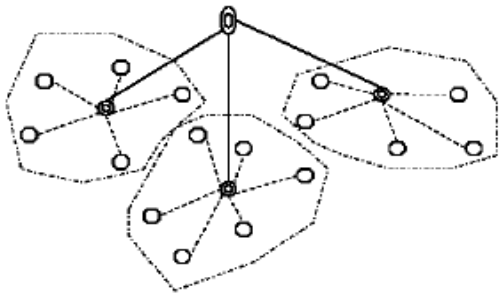

Fig. 7. Network architecture of clusters.

ferent schemes for unicast and broadcast information. However, our chaotic scheme can meet the needs of both at the same time.

Cluster heads within the same hierarchy form higher hierarchy clusters, so all the nodes in a higher hierarchy cluster also need to maintain a synchronous system. Thus, the cluster head which belongs to many hierarchies needs to maintain more synchronous systems, which make it hard to implement and more likely to exhaust. Therefore, this paper only considers two hierarchy clusters. Of course, in some applications, some cluster heads may be unlimited to energy, and if so more hierarchies may be considered.

3.3. Secure protocol

Chaotic keys have high security, but they may take more resources for synchronization of chaos than traditional symmetry keys. In order to take advantage of their chaotic features, a secure protocol based on chaos is proposed. In the following, BS stands for Base Station.

Initialization

(1) BS chooses the node with the most energy in each cluster to be the cluster head, then authenticates and initializes nodes with the initial pairwise keys.

Node – BS: $E_{k_s}\{ID, N\}$, where k_s denotes the pairwise key shared between node and BS, ID is the identification of its own, N is a nonce.

BS – node: $E_{k_s}\{C_i, H, N\}$, where C_i is the number of the cluster it belongs to, H is the ID of the cluster head, N is the same nonce as that in the message from the node to BS, which is used for freshness authentication.

BS – cluster head: $E_{k_s}\{C_i, N, list\}$, where $list$ is the list of cluster members.

(2) The cluster head chooses an initial value and generates a chaotic system used as the key stream. Then, members within the cluster keep synchronization with it. After that, cluster head and members authenticate each other, each member encrypts its ID with a chaotic sequence key and sends it to the cluster head, and the cluster head decrypts with the synchronous chaotic sequence key and then responds.

Node i – cluster head: $E_k\{ID_i\}$, where k denotes the chaotic key generated by the sender i, every time k is different, but in the following the same k is used to

denote chaotic key for convenience.

Cluster head – node i: $E_k\{ID_i\}$.

(3) the cluster head distributes TDMA slots to each member and sends the TDMA information.

Cluster head – cluster members: $E_k\{ID_i, TDMA\}$.

(4) BS or Sink acts as a higher cluster head and all the cluster heads keep synchronization with it as members.

Communication process

(1) If a member has information to send, it generates two segments of the chaotic sequence, the first is used as encryption key K and the latter as chaotic message authentication code (CMAC), i. e., the key K'.

(2) Plaintext is computed by exclusive OR operation with an encryption key and the ciphertext is generated. Then, the whole or part of the ciphertext operate exclusive OR with a CMAC key, which is sent to the cluster head together, i. e.,

$E_k\{D\}, CMAC(K', E_k\{D\})$,

where K is the chaotic encryption key, K' is another segment of the chaotic sequence used as message authentication code (MAC), CMAC denotes chaotic MAC, the effect of which is the same as the conventional MAC. For message integrity authentication, the receiver can first decrypt CMAC and then compare it with ciphertext $E_k\{D\}$: if same, then the message is not altered.

(3) The cluster head receives a data packet and decrypts it with the synchronous chaotic key and CMAC key, authenticates the message integrity, and decrypts the data packet.

(4) The cluster head may receive many data packets, so it will aggregate data information before sending to the next hop.

(5) Each cluster head acts as a cluster member in a higher cluster and encrypts data with chaotic keys of the new chaotic system, the process of which is the same as in the lower cluster.

(6) Data packets are forwarded through a hierarchy of cluster heads till they reach the sink.

Reelection of cluster head

When the energy of a cluster head falls below some threshold, it queries all nodes in its cluster and chooses the node with the most energy to be a new cluster head, and then broadcast the result to all its members. Synchronization of the new head with other heads is completed by BS.

The cluster head broadcasts query packet: $E_k\{requir\_en\}$.

Each member answers to the remainder energy: $E_k\{en\}$.

The cluster head chooses a new head and sends the result to all members as BS.

Cluster head – new head: $E_k\{list\}$.

Cluster head – members: $E_k\{H_n\}$, where H_n is the ID of the new head.

Cluster head – BS: $E_{k_s}\{H, H_n, C_i\}$, where H is the ID of the old cluster head.

New head – BS: $E_{k_s}\{H_n\}$.

BS validates the new cluster head by comparing H_n in notifying message of the old head and ID in authentication message of the new head. Then, it makes the new head synchronous with the others.

4. ANALYSIS

4.1. Performance of keys

(1) Secure analysis of chaotic keys

Chaotic system in this paper is able to provide a large key space, so it is sufficient for encryption of WSN. Logistic and tent maps are a kind of simple and widely used chaotic map functions, the performance of which has been fully proved. The N-Logistic-tent map is based on these two simple maps, and its chaotic features are proved to be better than the two basic maps, thus the performance of the N-Logistic-tent map can directly apply to our scheme, that is, the ciphertexts are completely different with different keys. By checking the binary sequence generated by the chaotic encryption system, we find that the distribution of 0 and 1 is well-proportioned and accord with random-number characteristics, so the sequence can be regarded as a random sequence. Moreover, its statistic features change a lot of after encryption.

Since chaotic encryption belongs to stream mode, attacks to block ciphers are useless. Chaotic signals are undirectional and generated by iterations. After the exclusive OR operation, the forecast of key stream is almost impossible, so it can resist plaintext and ciphertext attacks. Chaotic encryption keys are more robust than conventional symmetric keys. Once symmetric keys are captured, an attacker can encrypt data and send spoofed messages. While chaotic keys are different every time, unless the whole chaotic system is broken, the capture of a single chaotic key is insignificant.

(2) Cost analysis

WSN have limited energy, computing capability and memory, so the cost of the encryption algorithm is important. Cost of the chaotic encryption system includes time cost and space cost. And time cost also falls into two parts, preparing time and encrypting time. Commonly, preparing time before encryption is used to generate keys, and encrypting time means the time of encrypting plaintext with keys. Chaotic encryption belongs to stream mode, so its preparing time is very short, and the encrypting time is also shorter than block-cipher systems because during this time only exclusive OR is executed. Especially, the map in our scheme is a simple chaotic function, solving the equation is easy, so the complexity is small and the encryption speed is high. Space cost includes solid space and running space. Solid space is the space occupied by the code, and running space is the temporary space needed when running the algorithm. As seen from the equation, the code space is small. Since there is no s-box space in the chaotic encryption algorithm, temporary variables are few, the register variables in the process of cycling are also limited, and the map in this scheme only needs simple iterations, so running space is also small. To conclude, the cost of this chaotic cryptosystem is low.

However, the chaotic map we choose is a very simple one, so its security may be weaker than other complex ones. But WSN resources is very limited, so the simple strategy is a tradeoff between resources and security.

4.2. Performance of secure protocol

(1) Security of the protocol

1) Each time a data packet is encrypted, where the chaotic key is different, so the ciphertext is also different. So semantic security is guaranteed.

2) Another segment of the chaotic sequence is used for message integrity, which is similar to the traditional MAC. If a message is altered, the decryption of CMAC will be different from the ciphertext of data, so this scheme can defend against information altered attack.

3) Chaotic keys are different each time, and the receiver decrypts by using synchronous chaotic signals, so freshness is naturally guaranteed without nonce as in conventional schemes.

4) The initialization is completed by BS, and after clustering, cluster head and its members also authenticate each other, so a malicious node is hard to join.

5) The reelection of cluster head is also validated by BS, a malicious node can pretend to be a cluster head only when it has both chaotic keys within its cluster and the pairwise key shared with BS.

6) However, this scheme cannot resist node capture.

(2) Cost of protocol

A node communicates with BS by the pre-distributed pairwise key, so the cost of computing and memory are both low. In addition, the initialization is established only once when a network is deployed.

In the process of data communication, since chaotic encryption only needs exclusive OR operation, the computing complexity is small. There is no other additions to data packets except the CMAC part. The main cost only lies in the maintenance of the chaotic system. Therefore, the overall cost of the proposed secure protocol is low.

5. CONCLUSION

This paper has presented an N-Logistic-tent map and a secure cluster protocol for WSN. The N-Logistic-tent map is extended from the basic Logistic and tent maps, but the data range is enlarged, a parameter β is also added, and the value range of parameter μ to be chaotic is also enlarged, which together enhance the security. The secure protocol is based on cluster architecture and adopts both conventional symmetric encryption and chaotic encryption. In the process of initialization, nodes communicate with BS with pairwise keys, while in the process of data forwarding, chaotic encryption is used. In addition, a CMAC is designed by using chaotic encryption which has the same effect as the traditional MAC. All nodes in a cluster share a chaotic system and this kind of ciphers can encrypt broadcast packets as well

as unicast packets. Analysis has shown that the protocol can guarantee confidentiality, authenticity and freshness of information. Chaotic encryption is more secure than conventional symmetric schemes, insusceptible to disclosure, with a lower cost. So we have improved the security of a WSN protocol with low cost. Our future work includes further reducing the cost of the protocol, especially the cost in chaos synchronization. Finally, this scheme cannot resist node capture, therefore, how to improve this should also be further studied.

ACKNOWLEDGEMENT

This work was Supported by the Technology Key Task Program of Heilongjiang Province (No. GC02A121) and by the Science and Technology Projects of Heilongliang Provincial Education Department (No. 10531131).

(Received September 30, 2007.)

REFERENCES

[1] G. Huang and Y. Zhou: MANET security communication model based on multistage chaotic encryption. Comput. Engrg. Appl. *3* (2006), 136–139.
[2] K. Kelber: General design rules for chaos-based encryption systems. Internat. Symposium on Nonlinear Theory and its Applications *1* (2005), 465–468.
[3] S. Liu, F. Liang, and G. Xin: Chaos and Fractal in Natural Science. Beijing: Publishing House of Beijing University 2003, pp. 16–53.
[4] J. Luo and H. Shi: Research of chaos encryption algorithm based on logistic mapping. In: Internat. Conference Intelligent Information Hiding and Multimedia Signal Processing 2006, pp. 381–383.
[5] J. Lv, J. Lu, and S. Chen: Chaos Time Series Analysis and its Applications. Wuhan: Publishing House of Wuhan University 2002, pp. 72–92.
[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar: SPINS: Security protocols for sensor networks. Wireless Networks *8* (2002), 5, 521–534.
[7] G. Plitsis: Performance of the application of chaotic signals in IEEE 802.11b and wireless sensor networks. In: Proc. Seventh IEEE Internat. Symposium on Computer Networks. 2006.
[8] Y. Wang, G. Attebury, and B. Ramamurthy: A survey of security issues in wireless sensor networks. IEEE Comm. Surveys & Tutorials *8* (2006), 2, 2–23.
[9] H. Yu, P. Zeng, and W. Liang: Intelligent Wireless Sensor Network System. Beijing: Publishing House of Science 2006, pp. 126–132.
[10] C. Zhu and Z. Chen: A fast combined chaotic cryptographic method fitting mobile computing. Comput. Engrg. *31* (2005), 1, 138–140.

Qian Fang and Xiaoqun Zhao, School of Electronic & Information Engineering, Tongji University, Shanghai, 200092. China.
e-mail: xian17216@sina.com

Ying Liu, School of Electronic Engineering, Heilongjiang University, Harbin, 150080. China.
e-mail: eagle9607@sina.com