International Journal of Engineering & Technology, *7 (3.4) (2018)* 223-230

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure Group Communication in WSN based on Integrated approach of Chaos and Neural Network

H S Annapurna [1]*, M Siddappa [2]

[1]Dept. of Computer Science & Engg., Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India.
[2]Professor and Head, Dept. of Computer Science & Engg.,
Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.
**Corresponding author E-mail- hsassit@gmail.com*

Abstract

With advancement in technology, at present, there is possibility to develop low cost sensors in the area of wireless sensor network. Often in practice, there are huge numbers of sensors, which are deployed in hostile environment. Hence, there is a need to develop the security mechanism so that defined applications can serve the purpose. Two areas come under security consideration, protection for communication data and authentication of communicating parties. In this paper, chaos and neural network based centralized security mechanism has been developed. Two different types of chaotic maps, Lozi and Logistic maps have been integrated with feed-forward architecture of neural network to deliver the security provision. The sensitiveness with initial conditions of chaos has been exploited for key development. Proposed method not only provides high level of security but also carries high level of flexibility, scalability and computational efficiency.

Keywords: Chaos; Logistic map; Lozi map; Neural Network; Wireless Sensor Network.

1. Introduction

Recent trends in microprocessors and wireless communications have empowered the extensive deployment of sensor systems involving little sensors which have detecting, correspondence, and calculation capacity over a huge recorded to get document grained detecting information. Some of the main application areas of sensor networks are military target tracing, exact agriculture, living space observing, condition control and so on. Following the developments of winged creatures and bugs, observing natural conditions that influence yields and domesticated animals and so forth., come under environmental applications of sensor networks. Data-centric information broadcasting becomes the most vital task for the sensor network in which the sensors send the sensed data as a response to the queries sent by the applications. Wireless Sensor Networks (WSNs) comprise of an enormous number of sensor nodes which are installed in an unattended unfriendly area. Every sensor node needs to detect particular events and report the sensed data to the central node (base station). Sensor nodes have to meet their objectives with marginal memory utilization, energy depletion, communication and calculation cost due to their restricted physical resources. Further, sensor nodes may have to self-organize into clusters in a collaborative manner for the collection of particular information or for the achievement of a specific task. Sensor nodes are exposed to a extensive series of attacks since they are deployed in an unattended area which has no physical security, human intervention and since they have to communicate with wireless connection. Therefore, sensor-oriented applications need to be secured. Particularly in group-oriented applications, information exchanged among the members of the group requires greater level of protection. In military applications, for example, group of sensor nodes cooperate with each other to track a target and may interchange information pertaining to the location of this target. If an adversary injects junk data in to the network, it may disrupt the operation of network. In medicinal applications as well, patient's biological factors gathered by a collection of sensor nodes must be maintained secured and confidential. Secure Group Communication (SGC) plays a very important role in providing location confidentiality which is of greatest concern in military, motherland security and environment monitoring applications. Subsequently, a SGC scheme must be employed to make the data transmission within the group secure and to provide protection against probable attacks. In conventional networks, SGC problems have been addressed and many schemes have been designed for SGC. Inborn characteristics of WSNs make the problem of addressing SGC a challenging issue. Several schemes have been proposed since a decade for SGC in WSN. These schemes can be broadly classified into three types: Centralized, Decentralized and Hybrid approach. In the first approach, a central trust element is responsible for managing the group. Particularly, it needs to handle the membership change events and is responsible for rekeying operations. In the decentralized approach, all members of the group contribute for the management of the group instead of assigning the work to a central element. The contributory approach has the benefit of failure-tolerance over centralized approach but has computational overhead. In the hybrid method, the task of managing the group is collaboratively shared between the central entity and the group members which provides both efficiency and failure-tolerance. Two main components of SGC scheme are the managing the group key and the group membership. Among them, managing the group key is the fundamental problem of SGC. In this paper, we provide a solution to the problem of group key computation and management for SGC in WSN using an integrated approach of neural networks and chaotic maps (CHNNSGC). The remaining part of the paper is sorted out as

follows: We discuss the work related to SGC in Section 2. Section 3 briefs about chaos theory and its applications. Section 4 presents a proposed solution followed by experimental analysis in section 5. We conclude our work in section 6.

2. Related Work

To handle the challenges of secure group communication, several works have been done in the past. A Group Key Agreement (GKA) scheme is needed for setting up a group key with all the members belonging to the group over a public network. The scheme poses a major challenge in secure and proficient group communications. Contributory Group Key Agreement (CGKA) protocols are more appropriate for dynamic groups. [1] has proposed a secure CGKA scheme based on ring structure. As a part of member join or leave operation, there are many strategies about secure communication and exact verification. Furthermore, the concerns about passive attack, obscure key-share, key newness, contributiveness, backward confidentiality and forward confidentiality have been discussed. The problem of reliable communication within a group on the network layer has been discussed in [2]. A safe overt multicast routing technique called Xcastor has been designed and implemented by the authors in which they enhance the secure and adaptable routing idea of the Castor unicast routing technique to support consistent data transmission among large numbers of small groups. In [3] authors have proposed an architecture for group-oriented communication which is secure and reliable. The architecture makes use of cryptography based on NSA Suite B and may be suitable for handling delicate and DoD classified data up to SECRET. In [4], the authors have proposed a scheme for achieving secure communication within a group which is designed using Chinese Remainder Theorem to provide both confidentiality and non-repudiation features. In this scheme, all the members belonging to a group provide their own public keys to draw a shared public key used for encryption. Both confidentiality and non-repudiation have been achieved through the shared public key and the corresponding secret key. In [5], the requirements of efficiency, and security have been satisfied by proposing a scheme called Dynamic Access Control Scheme (DACS). In particular, the scheme offers the some of the benefits such as computation of the hash function only once by every sensor node and gaining access to the group key during initialization phase or during maintenance phase. In [6], authors have proposed an effective secure group communication scheme by considering a group of nodes sensing the similar kind of data. The scheme facilitates group management and group key distribution in a secure manner. The scheme uses a logical ring structure, which alleviates the job of the group controller in managing the key used for communicating within a group. The scheme also offers backward and forward confidentiality, talks the problem of node compromise attack and detects and evicts the compromised nodes. [7] has focused on trade-offs between communication cost and storage cost and rekeying cost for secure multicast and presented a set of algorithms for the same. A key management technique using a geometric approach is proposed in [8] for achieving secure group communication. In the proposed technique, members of the group compute the group key by solving a set of linear equations. This is done by making use of public information on the notice board as well as their own secret information. [9] has proposed a security mechanism for secure communications in clustered networks. A group of sensor nodes sharing the same sensory information is defined as a group. The main objective here is to provide access to the group information solely to the authorized members of the group. Key assignment protocol which is self-healing is proposed in [10] for multicast communications in wireless network scenario. The scheme offers a method for sending rekeying messages securely and discusses the techniques for membership change events. Hashing and XOR operation are performed for sending the rekeying messages and the lost session keys are recovered by the nodes on their own without requesting it from the group controller. In [11], the authors have proposed a technique for secure group rekeying in WSNs with the eviction of the compromised nodes. This scheme handles member join and leave events in a group. Exclusion of a compromised node is a key issue in WSNs because of their exposure to threats. The main focus in the proposed technique is on exclusion of traded off nodes from a group without performing re-grouping. Once a node is compromised, it is expelled from the group and it is not allowed to enter any group later. In [12], the design of hierarchical group key circulation scheme which is self-healing is discussed for WSN of heterogeneous type. They have set up a prototype for hierarchical group key circulation and the proposed scheme is secure and computational efficient. [13] has proposed a model that allows secure one-to-many communication for limited capability networks in the face of a strong attacker which can capture an random set of nodes. Focus is given over two main modules: group key establishing protocol and distinct key management. [14] has presented a light-weight Key Freshness method which makes use of XOR operations in which the key is refreshed without transmitting messages between the nodes. The group controller sends a single message consisting of a magic word to the members of the group and XOR and left shift operations are performed for refreshing the keys. Group key management scheme for heterogeneous WSN has been discussed in [15] which is based on LKH++. The management of group key is carried out dynamically by constructing a secure key tree. The encryption, communication and storage overhead are analyzed individually for head of the cluster and member of the cluster for node addition/eviction operations and are logarithmic in nature. AKMS [16] presents authentication and key management protocols for WSN to provide authenticity and message secrecy among mobile sensor nodes using a combination of HMAC and Elliptic Curve Cryptography with low energy requirement. In [17] detailed study and classification of different schemes for secure group communication is discussed. The analysis and performance of existing schemes in terms of both key management and membership management in a group has been presented. [18] presents a scheme for key management based on LKH protocols which reduces the rekeying costs by exploiting the topological information of the network. Three different protocols are discussed which are suitable for different applications. A basic scheme with no network key and no cluster overlap which offers minimal rekeying cost, second scheme with cluster overlap which offers scalability but with higher rekeying cost and the third scheme which aims at providing a group communication scheme by adding a network key to the basic scheme.

3. Chaos Theory

The theory of chaos denotes the mathematical models which have the ability to produce chaotic shapes in consecutive values of the dependent variables. Chaos theory find its application in various engineering disciplines. An important function of chaotic schemes is that little changes in the initial values may result in enormously unpredictable future behaviors. This sensitive dependency on initial settings is normally shown by schemes having several entities with nonlinear interactions and it is observed not only in complex systems, but also with linear models. Chaotic systems can be treated as qualitative even in the simplest logistic equation. By nature, they are nonlinear and can be well delineated by studying unstable, aperiodic actions in deterministic nonlinear dynamical arrangement. By this description, many significant facts concerning the features of chaos can be drawn. First of all is that chaos system is dynamical in nature which means that it varies with time. Second is that the behavior of the chaos models are not periodic and not stable. Third is that even though chaotic performance is multifaceted, it can take simple reasons via deterministic procedure. Fourth is that because of the nonlinearity of the system, it is sensitive to initial conditions meaning that with different initial parameters , two statistically uncorrelated logistic arrangements are generated. Fifth is that chaotic behavior is not

unsystematic, since the system is deterministic. Even though it is deterministic, the performance of chaotic schemes is unpredictable since it is unstable, aperiodic and sensitive to initial conditions,. Final characteristic of chaos is that the current output becomes the input for next iteration. Mathematically, chaotic map can be defined as a map that shows some type of chaotic behavior. In our work, we consider two types of chaotic maps: Lozi map and Logistic map.

3.1. Lozi Map

A new chaotic approach is discussed here which is based on Lozi map. Lozi map is simplification of the He´non map with the term $-P(X(t))^2$ is replaced by $-P|(X(t)|$ and it admits numerically strange attractor for (P,Q) = (1.7,0.5). This map which is chaotic in nature also includes functions that are not differentiable. As a result the modeling of the associate time series is made difficult. The Lozi map is specified by the equations (1) and (2).

$$X(t+1) = 1 - P.|X(t)| + y(t) \quad (1)$$

$$y(t) = Q.X(t) \quad (2)$$

Here,'t' is the repetition number. In this work, the values of y are stabilized in the range [0, 1] to each decision variable in n-dimensional space of optimization problem. This conversion is given by equation (3).

$$Z(k) = \frac{y(k) - \lambda_{min}}{\lambda_{max} - \lambda_{min}} \quad (3)$$

where y ϵ [-0.6418, 0.6716] and [λ_{max}, λ_{min}] equals to [0.6418, -0.6716]. The values used in our work are P=1.7 and Q=0.5. These values are sensitive to initial conditions. The experiments are carried out for two dissimilar initial settings and resulting chaotic sequences are shown in Fig.1 below.

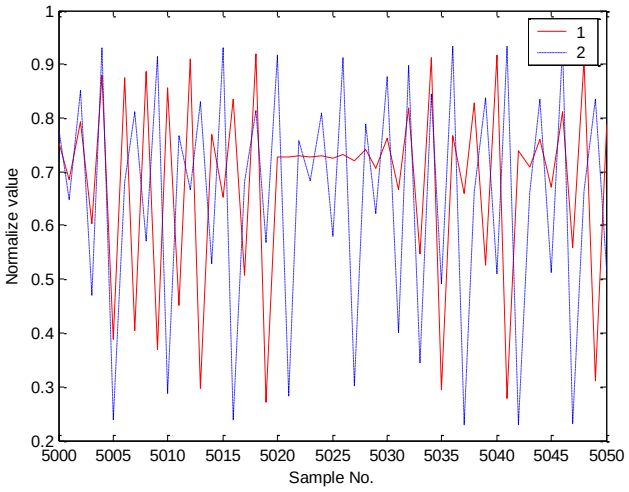

Fig.1: Sensitivity of chaotic sequence with initial condition in Lozi map

In Fig.1 first set of data is generated with initial values for X = 0.457, y=0.053 whereas second set of data is generated with initial values for X= 0.407, y=0.242. The generated variations between two chaotic sequences are shown in Fig.2 for 50 samples. As we can see in the figures, there is a very substantial difference between these two chaotic sequences which creates a very difficult environment for an adversary to make a guess on parameters of initialization and results in more robust solution.

3.2. Logistic Map

Logistic map can be explained as in equation (4).

$$S[t+1] = \lambda * S[t][1 - S[t]] \quad (4)$$

where λ is a positive constant sometimes known as the biotic potential. The values of interest for the parameter λ are those in the interval [0, 4]. This quadratic map behaves diversely and dependent on the value of λ. If $1<\lambda<3$, the fixed point for the equation is defined as $S=1-\lambda^{-1}$. For $\lambda=3$, system branches to give a cycle of period two which is stable for $3<\lambda<1+6^{0.5}$. Fig. 2 below shows chaotic sequences generated for two different values of $\lambda=3.679$ and $\lambda=3.737$ and initial condition S(0)=0.2.

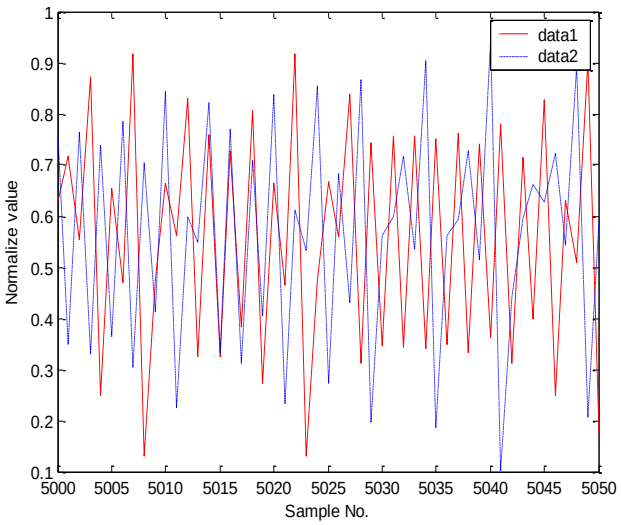

Fig.2: Sensitivity of chaotic sequence with initial condition in Logistic Difference equation

4. Proposed Solution

As there is a need to establish a secure communication in the group, here we have proposed an integrated approach of neural networks and chaotic maps as a solution to the problem of group key computation and management for SGC in WSN. This integration will provide a compact form of personal and group key. The generated key will be a combination of neural network weights and various initial conditions for chaotic maps. We discuss the proposed solution in two phases.

A. Chaotic map samples generation for SGC

B. Secure Message Generation

A. Chaotic Map Samples Generation for SGC

Chaotic samples are generated through both Lozi and Logistic equations which will be utilized to secure the message and will define the key information. After defining the initial conditions, the required number of samples is estimated and chaotic samples are generated. Samples generated through Lozi map are further normalized using Eq.3 so that samples could confine in the range [0, 1]. Thus, samples generated from Lozi and Logistic maps are used in two forms in real form as it appears after normalization and digitized form to secure the message. The complete process of chaotic samples generation from Lozi and Logistic equations is shown in Fig. 3 and Fig. 4 respectively.

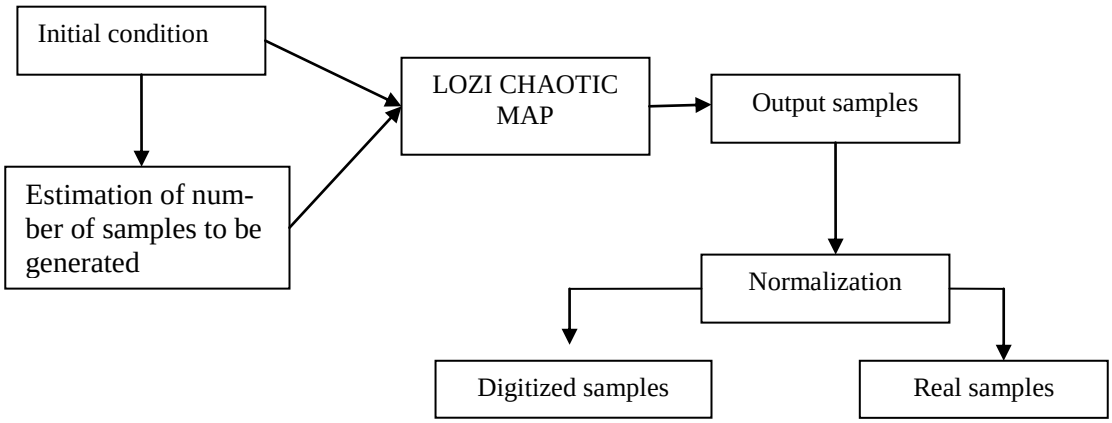

Fig.3: Samples generation through Lozi map

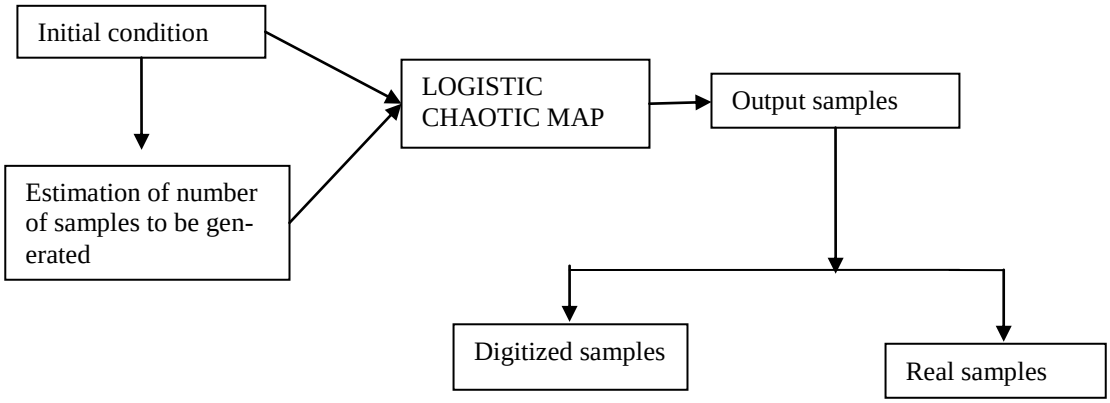

Fig.4: Samples generation through Logistic map

Thus the samples generated from Lozi and Logistic maps are used as training data for neural network. The neural network weights together with the initial conditions for chaotic maps which are selected through uniform random process contribute to personal and group key formation. The group keys are distributed to individual sensor nodes by the sink node using the personal keys in an additive manner. The key formation process is illustrated in fig. 5 below.

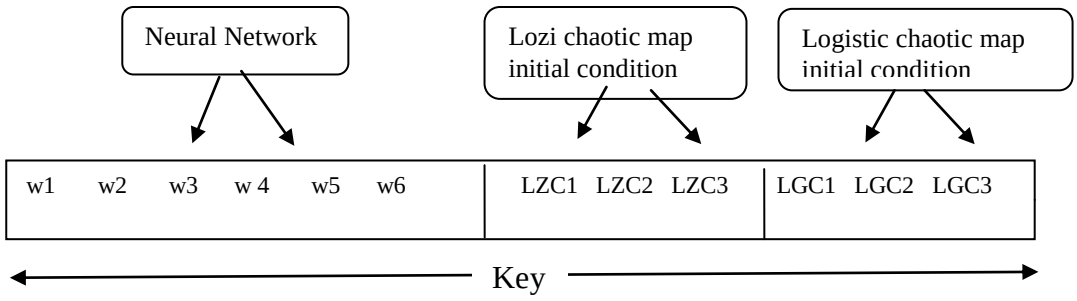

Fig.5: Key formation process

The whole process of personal key generation and group key generation is shown below.

Personal Key Generation

N = Number of members in the Group
FOR i = 1: N
TRD ← Load the Training data to neural network;
T ← Assign target;
PMW (i) ← [(NN(TRD))→ T] ;
PLZ (i, 1) ← Generate a random sample through U [M1 M2];
PLZ (i, 2:3) ← Generate two random sample through U[0,0.5];
PLZ (i, 4) ← Generate a random sample through U [R1 R2];
PLZ (i, 5) ← Generate a random sample through U [0.1 0.2];
PLZ (i, 6)← Generate a random sample through U[3.58,3.95];
Assign PMW (i) & PLZ (i, 1: 6) to the i^{th} member as personal key
END

Group Key Generation

TRD ← Load the Training data to neural network;
T ← Assign target;
GMW (i) ← [(NN(TRD))→ T] ;
GLZ (1) ← Generate a random sample through U [M1 M2];
GLZ (2:3)← Generate two random sample through U[0 0.5];
GLZ (4) ← Generate a random sample through U [R1 R2];
GLZ (5) ← Generate a random sample through U [0.1 0.2];
GLZ (6)← Generate a random sample through U[3.58,3.95];
STORE GMW & GLZ as the Group key and distribute it to every member.

B. Secure Message Generation

To secure the message, the neural network weights and initial conditions of both chaotic maps are extracted from the group key. Using the initial conditions, chaotic samples are generated through Lozi and Logistic equations. The Lozi samples are normalized and the discrete version of these normalized samples are XORed with the message to be secured. The result is further XORed with discrete version of Logistic samples. The continuous samples from both the maps are applied to neural network as inputs. Output of the neural network after architecture processing is converted to discrete form and XORed with previous XOR output to form the secure message. The whole process of securing the message communicated in the group is represented in Fig.6. The complete protocol for secure group communication is shown in Fig.7.

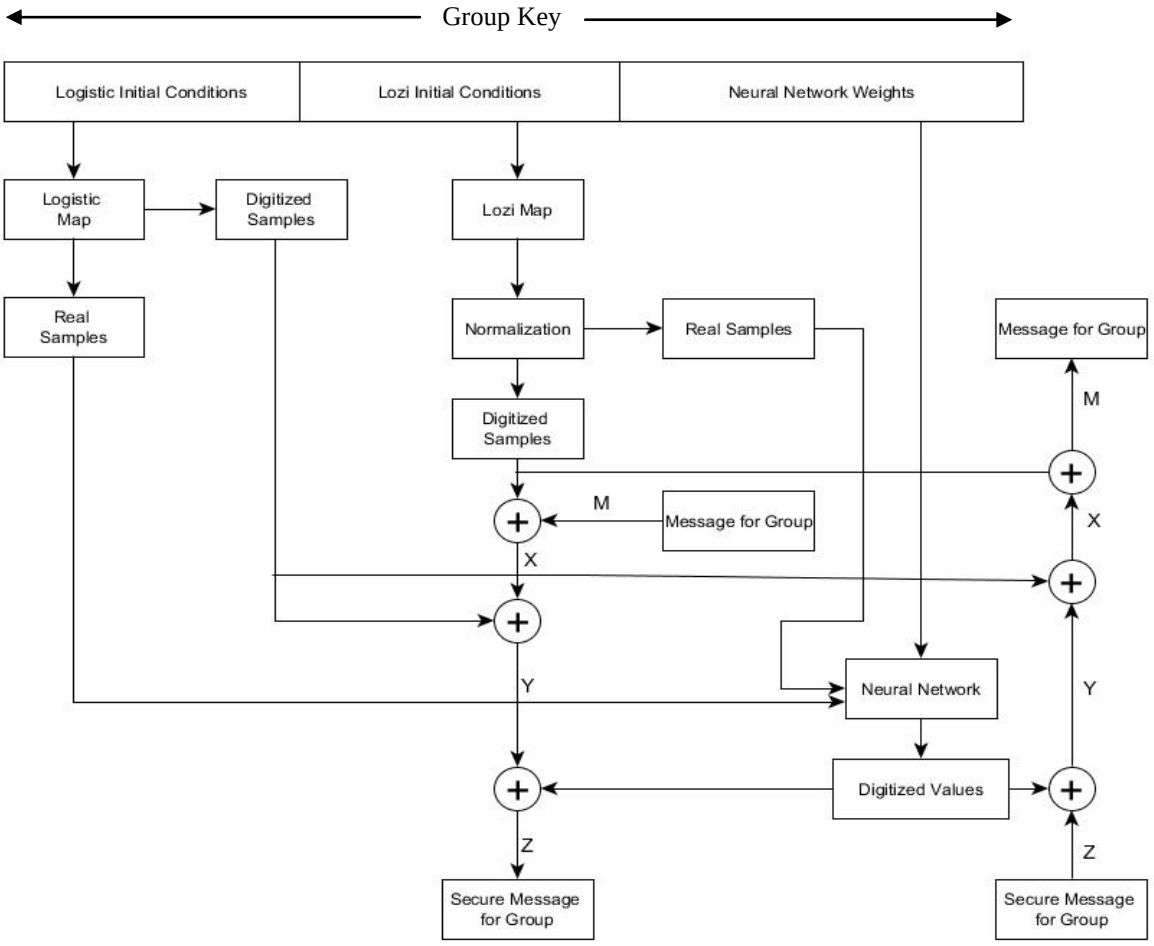

Fig. 6: Generation and Interception of Secure Message for the Group

Protocol for Secure Group Communication

1. Initialization of Group size.
2. Assign the personal key to each member of the group.
3. A group key is generated and distributed to all the group members using personal key in an additive manner.
4. Communicate the message securely to group members through group key.
5. Group members intercept the message through group key

Protocol for member join event

1. Resize the group.
2. Assign a personal key to new member.
3. Generate a new group key.
4. Secure the new group key through personal key in an additive manner and distribute the same.
5. Each group member extracts the new group key by subtracting its personal key.

Protocol for member leave event

1. Resize the group.
2. Discard the personal key of the leaving member.
3. Generate a new group key
4. Secure the new group key through personal key in an additive manner and distribute the same.
5. Each group member extracts the new group key by subtracting its personal key.

Fig. 7: Secure Group Communication Protocol

5. Experiment Analysis

For the experiment point of view, messages of different lengths have been considered and the quality of the proposed method is investigated through key variations over the complete process. Whole process has been developed under MATLAB environment. A feed-forward architecture of size [2:2:1] is used to develop the neural network. Random samples from Lozi and Logistic maps are used as training data for the neural network. Steepest decent method has been applied to train the neural network. For a group with 5 members developed personal keys and group keys are shown in Table 1 and Table 2 respectively.

Table 1: Personal key information

Group member	Neural Network Weights	Chaotic Initial condition
1	[0.6199 0.6170 0.2647 0.0039 0.5228 -0.2397]	5.561100000000000e+004 4.324647962803379e-002 1.277814036163683e-001 1.146500000000000e+004 1.383863307924869e-001 3.943553475139261e+000
2	[0.4610 0.8517 -0.2999 0.4117 0.3577 0.2796]	3.136300000000000e+004 7.137053880584793e-002 1.386453791432110e-001 8.210000000000000e+003 1.891409540276523e-001 3.921027403633765e+000
3	[0.4219 0.7146 -0.0201 0.3852 0.6040 0.0181]	4.277500000000000e+004 3.882223682937964e-001 3.539907081103451e-001 1.253600000000000e+004 1.407792408898110e-001 3.750904693789188e+000
4	[0.3526 0.7440 0.2749 0.5474 0.9853 -0.2374]	6.846700000000000e+004 3.014616253829622e-001 1.970949551993544e-002 1.080300000000000e+004 1.376830393625589e-001 3.787742756045565e+000
5	[0.7813 0.2855 -0.1339 0.3493 0.8200 0.1359]	5.665600000000000e+004 4.228408046763044e-001 1.148706458546724e-001 1.337300000000000e+004 1.088449591792891e-001 3.762553921246980e+000

Table 2: Group key information

Time	Neural Network Weights	LOZI Initial Condition	LOGISTIC Initial Condition
0.1720	[0.5567 0.8790 -0.1427 0.8888 0.6823 0.1393]	6.219100000000000e+004 3.499079641027891e-001 2.053739502195478e-004	9.995000000000000e+003 1.170788464764357e-001 3.655196765923339e+000
MESSAGE INFORMATION : 1 1 1 0 0 1 0 1 0 1			
SECURE MESSAGE: 1 0 1 0 0 1 0 0 1 1			
INTERCEPTED MESSAGE: 1 1 1 0 0 1 0 1 0 1			
TIME TAKEN IN SECONDS FOR SECURING/INTERCEPTING MESSAGE INFORMATION : 0.0150			

For a message of length 10 bits , the secure message generated by the sending group member and message intercepted by the receiving group member are shown in Table 2.Time involved in securing or intercepting the message is 0.015 seconds. For the sensitivity analysis, three different forms of attacks have been applied.

(i) Assuming that only neural network weights are unknown while chaotic initial conditions are known.

(ii) Assuming that only Lozi initial conditions are unknown.

(iii) Assuming that only Logistic initial conditions are unknown.

Sensitivity of the message with respect to small changes in the neural network weights, Lozi initial conditions and Logistic initial conditions of the group key is shown in Tables 3 to 5.

Table 3: Sensitivity for neural network weights

Secure Message	Neural Network Weights	Intercepted Message
1 0 1 0 0 1 0 0 1 1	[0.5567 0.8790 -0.1427 0.8888 0.6823 0.1393]	[1 1 1 0 0 1 0 1 0 1]
1 0 1 0 0 1 0 0 1 1	[0.1385 1.1074 -0.8073 0.8678 -0.3259 0.6975]	[1 1 1 0 0 1 0 0 1 1]
Sensitivity		20 %

Table 4: Sensitivity for Lozi initial conditions

Secure Message	Lozi Initial Conditions	Intercepted Message
[1 0 1 0 0 1 0 0 1 1]	6.219100000000000e+004 3.499079641027891e-001 2.053739502195478e-004	[1 1 1 0 0 1 0 1 0 1]
[1 0 1 0 0 1 0 0 1 1]	6.435100000000000e+004 3.029048668394501e-001 2.094752948354952e-004	[1 0 1 0 1 1 1 0 0 0]
Sensitivity		50%

Table 5: Sensitivity for Logistic initial conditions

Secure Message	Logistic Initial Conditions	Intercepted Message
[1 0 1 0 0 1 0 0 1 1]	9.995000000000000e+003 1.170788464764357e-001 3.655196765923339e+000	[1 1 1 0 0 1 0 1 0 1]
[1 0 1 0 0 1 0 0 1 1]	1.002200000000000e+004 1.601718615013891e-001 3.665631425869211e+000	[1 1 1 1 0 0 0 1 0 0]
Sensitivity		30%

Messages of different lengths have been taken independently and 10 trails have been applied to estimate the sensitivity for each case. The obtained results are shown in Table 6. It is evident from the results that on an average sensitivity is nearer to 50%. Sensitivity analysis confirms that the secure message cannot be intercepted by any evicted member who tries to access the message with old group key as illustrated in Table 7.

The proposed work is compared with previous works carried out in the area of secure group communication and their algorithmic characteristics are shown in Table 8. Small key size, easy means of key changing and high level of uncertainty in outcome prediction make the proposed method very competitive and useful.

Table 6: Sensitivity with variations in neural network weights and initial conditions

Trial No.	10 bits	50 bits	100 bits	1000 bits
1	[50 40 40]	[58 38 28]	[44 37 35]	[42 30 32]
2	[50 30 40]	[58 28 36]	[44 40 37]	[53.4 27.9 38.2]
3	[60 40 30]	[58 30 36]	[37 32 35]	[46.6 30.1 36.2]
4	[50 10 70]	[42 26 44]	[29 34 31]	[46.8 28.6 40.5]
5	[70 20 30]	[42 30 42]	[44 72 30]	[46.6 30.5 38]
6	[50 20 40]	[58 34 16]	[44 39 39]	[54.8 37.4 28.6]
7	[40 30 60]	[58 36 28]	[56 72 32]	[29 77.9 37.7]
8	[30 40 50]	[56 30 26]	[56 35 41]	[53.4 29.5 38.7]
9	[50 60 50]	[58 40 22]	[58 32 38]	[46.8 28.9 36.1]
10	[50 30 40]	[58 40 30]	[39 39 38]	[46.8 28.9 38.8]

Table 7: Resource accessing after exclusion

Secure Message	[0 0 1 1 1 1 0 0 1 0]	Intercepted Message
New Group Key after exclusion of member	[0.7804 0.7380 -0.2473 0.3433 0.1110 0.2611] 3.373500000000000e+004 4.643942024280887e-001 2.425679189420351e-001 9.142000000000000e+003 1.276342055462411e-001 3.628460278025710e+000	[1 0 1 1 0 1 0 0 1 0]
Old Group Key before exclusion of member	[0.5567 0.8790 -0.1427 0.8888 0.6823 0.1393] 6.219100000000000e+004 3.499079641027891e-001 2.053739502195478e-004 9.995000000000000e+003 1.170788464764357e-001 3.655196765923339e+000	[1 1 1 0 0 0 0 0 0 1]

Table 8: Comparative Performance Analysis

Scheme	Storage cost At GC	Communication Cost	Computation cost	Cryptographic type	Key update
SGCHS (Kauser et.all:2007)	Very High: O(n+m) (*n* symmetric keys+*2.m* keys+ *m* rnd)	Low for rekeying, O(1), one broadcast message sent, High for each Join event: O(m)	Low (XOR and Hash function	XOR & Hash function are used in rekeying)	Periodic
SGR (Khalid 2009)	Very high : O(n+m) (random number of symmetric keys proportional To the number of group members and two hash chains:2m keys)	Low for rekeying, O(1),one broadcast message sent, High for each Join event: O(m)	Medium: O(*l*) hash + polynomial computation	polynomial+μTESLA	Periodic
HSHKD (Yang:2009)	Very high O(2.m+m.(t+1)) where t is polynomial degree	Very high: O(2(t+1))	High: O(2t) multiplication	polynomial	Periodic
SBSA (Szalachhowski:2015)	High O(n)	High O(n)	High O(n) Encryption on GC	Symmetric and pseudo-random generation.	At membership change
XKPS (Ghafoor:2015)	High O(n)	High O(n)	High O(n) Encryption on GC	Symmetric, Hash function, and XOR	At membership change
CHNNSGC	Low: Linear increment with n	Low for rekeying, O(1)	Very Low (Initial conditions of chaotic map & weights of NN)	Chaotic maps, NN and XOR	At membership change

6. Conclusion

The need for secure group communication has become obvious instead of requirement at present. In this research paper, a very innovative method is proposed for group key computation and management to provide SGC in WSN. Proposed solution provides high level of security at the same time a very comfort zone to change the key whenever it is needed using hierarchical approach of neural network and two different varieties of chaotic maps. Proposed method requires a small key size and it carries very high level of sensitivity with a very small change in key information.

References

[1] Yu-Yi Chen, Chuan-Chiang Huang, Jinn-Ke Jan,"The Design of Secure Group Communication with Contributory Group Key Agreement Based on Mobile Ad Hoc Network ", *International Symposium on Computer, Consumer and Control (IS3C)* ,Year: 2016 Pages: 455 - 460, DOI: 10.1109/IS3C.2016.121

[2] Milan Schmittner, Matthias Hollick,"Xcastor: Secure and scalable group communication in ad hoc networks ", *IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*,Year: 2016, Pages: 1 - 6, DOI: 10.1109/WoWMoM.2016.7523512

[3] M. Tamer Refaei, Jeffrey Bush, "Secure Reliable Group Communication for Tactical Networks ", *IEEE Military Communications Conference*, Year: 2014, Pages: 1195 - 1200, DOI: 10.1109/MILCOM.2014.200

[4] Xixiang Lv, Hui Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks", *IET Information Security*, Year: 2013, Volume: 7, Issue: 2,Pages: 61 - 66, DOI: 10.1049/iet-ifs.2010.0314

[5] Fan Wu; Hao-Ting Pai; Xinxin Zhu; Pei-Yun Hsueh; Ya-Han Hu,"Dynamic access control for secure group communication in wireless sensor networks ", *The 8th Electrical Engineering/ Electronics, Computer, Telecommunications and Information Technology (ECTI) Association of Thailand – Conference*, Year: 2011 , Pages: 288 - 291, DOI: 10.1109/ECTICON.2011.5947829

[6] Omar Cheikhrouhou; Anis Koubâa; Olfa Gaddour; Gianluca Dini; Mohamed Abid,"RiSeG: A logical ring based secure group communication protocol for Wireless Sensor Networks ", *International Conference on Wireless and Ubiquitous tems* ,Year: 2010 ,Pages: 1 - 5, DOI: 10.1109/ICWUS.2010.5670431

[7] Bezawada Bruhadeshwar; Sandeep S. Kulkarni ,"Balancing Revocation and Storage Trade-Offs in Secure Group Communication ", *IEEE Transactions on Dependable and Secure Computing* ,Year: 2011, Volume: 8, Issue: 1 ,Pages: 58 - 73, DOI: 10.1109/TDSC.2009.27

[8] Lina Ge,"Geometric Approaches-Based Key Assignment for Secure Group Communication System ", *Second International Conference on Future Networks* ,Year: 2010 ,Pages: 415 - 419, DOI: 10.1109/ICFN.2010.51

[9] Olfa Gaddour; Anis Koubâa; Mohamed Abid ,"SeGCom: A secure group communication mechanism in cluster-tree wireless sensor networks ", *First International Conference on Communications and Networking* ,Year: 2009 ,Pages: 1 - 7, DOI: 10.1109/COMNET.2009.5373554

[10] Firdous Kausar,, Sajid Hussain,, Jong Hyuk Park,, Ashraf Masood,"Secure Group Communication with Self-healing and Rekeying in Wireless Sensor Networks, Mobile Ad-Hoc and Sensor Networks", *Volume 4864 of the series Lecture Notes in Computer Science* pp 737-748, 2007

[11] Asma Khalid,, Mukhtar Hussain,"A Secure Group Rekeying Scheme with Compromised Node Revocation in Wireless Sensor Networks, Advances in Information Security and Assurance", *Volume 5576 of the series Lecture Notes in Computer Science* pp 712-721, 2009

[12] Yanjiang Yang, Jianying Zhou, Robert H. Deng, Feng Bao, "Hierarchical Self-healing Key Distribution for Heterogeneous Wireless Sensor Networks, Security and Privacy in Communication Networks", *Volume 19 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* pp 285-295, 2009

[13] Pawel Szalachowski1, Tiffany Hyun-Jin Kim,"Secure broadcast in distributed networks with strong adversaries", Security and Communication Networks, Volume 8, Issue 18 ,Pages 3739-3750, Dec 2015.

[14] Ataullah Ghafoor , Muhammad Sher , Muhammad Imran Kashif Saleem,"A Lightweight Key Freshness Scheme for Wireless Sensor Networks", 12th International Conference on Information Technology - New Generations (ITNG), 2015.

[15] Wenbin Yao, Si Han, Xiaoyong Li, "LKH++ Based Group Key Management Scheme for Wireless Sensor Network", *Wireless Pers Commun*, DOI 10.1007/s11277-015-2582-0, 2015.

[16] Danyang Qin, Shuang Jia, Songxiang Yang, ErfuWang, Qun Ding, "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks", Hindawi Publishing Corporation, *Journal of Sensors*, Volume 2016, Article ID 1547963, 2016.

[17] Omar Cheikhrouhou, "Secure Group Communication in Wireless Sensor Networks", *Journal of Network and Computer Applications*, Volume 61, Issue C, 2016, Pages 115-132, DOI:10.1016/j.jnca.2015.10.011.

[18] Dimitris Tsitsipis, Anthony Tzes, Stavros Koubias, "CHAT: Clustered hierarchical key management for wireless sensor networks using network topology", *International Journal of Distributed Sensor Networks*, Year: 2017, Vol. 13(11) DOI: 10.1177/1550147717741570.