A Secure Key Predistribution Scheme for WSN Using Elliptic Curve Cryptography

Kishore Rajendiran, Radha Sankararajan, and Ramasamy Palaniappan

Security in wireless sensor networks (WSNs) is an upcoming research field which is quite different from traditional network security mechanisms. Many applications are dependent on the secure operation of a WSN, and have serious effects if the network is disrupted. Therefore, it is necessary to protect communication between sensor nodes. Key management plays an essential role in achieving security in WSNs. To achieve security, various key predistribution schemes have been proposed in the literature. A secure key management technique in WSN is a real challenging task. In this paper, a novel approach to the above problem by making use of elliptic curve cryptography (ECC) is presented. In the proposed scheme, a seed key, which is a distinct point in an elliptic curve, is assigned to each sensor node prior to its deployment. The private key ring for each sensor node is generated using the point doubling mathematical operation over the seed key. When two nodes share a common private key, then a link is established between these two nodes. By suitably choosing the value of the prime field and key ring size, the probability of two nodes sharing the same private key could be increased. The performance is evaluated in terms of connectivity and resilience against node capture. The results show that the performance is better for the proposed scheme with ECC compared to the other basic schemes.

Keywords: Key predistribution schemes, security, wireless sensor networks, elliptic curve cryptography.

Manuscript received Nov. 8, 2010; revised Apr. 20, 2011; accepted May 6, 2011.

Kishore Rajendiran (phone: +91 44 27474844/45/46, email: kishorer@ssn.edu.in), Radha Sankararajan (email: radhas@ssn.edu.in), and Ramasamy Palaniappan (email: ramasamy_18@yahoo.com) are with the Electronics and Communication Engineering Department, Sri Sivasubramaniya Nadar College of Engineering, Tamilnadu, India.

http://dx.doi.org/10.4218/etrij.11.0110.0665

I. Introduction

A sensor network consists of a large number of small, inexpensive, and self-powered devices that can sense, compute, and communicate with other devices. Nodes act as information sources, and sense and collect data samples from their environment. Wireless sensor networks (WSNs) have a wide range of civil and military applications. One of the important applications of a WSN is area monitoring, where nodes are deployed over a region to monitor an event or phenomenon. For example, in military applications, to detect intrusion in a battlefield, large quantities of sensor nodes are required along with high security. Similarly, WSNs can use different types of sensors to detect the presence or intrusion of vehicles ranging from motorcycles to armored fighting vehicles like tanks. Sensor networks are typically characterized by limited power supplies, low bandwidth, limited memory, and limited energy. When sensor networks are deployed, security becomes important because they are subject to different types of attacks. This leads to a very demanding environment to provide security. Although secure communication in a WSN is often an essential system requirement, it is a challenging task due to limited resources, lack of infrastructure, unknown topology, and wireless nature of transmission. To overcome this, many key predistribution schemes have been proposed. The aim is to assign a set of keys called a key ring to each sensor so as to enable any two sensors in a radio coverage area to establish a secure link and to maintain, at the same time, the network resiliency against node capture and key compromise.

Many key predistribution schemes failed to take into account the information on deployment location. However, prior deployment knowledge may be utilized to improve the performance of a random key predistribution scheme. Though

it may not be possible to previously know the exact location of a node, it is possible to have an idea about approximate location of a node after deployment. Several key predistribution schemes are developed in which a large pool of key is chosen and keys are assigned to each node randomly by selecting from the large key pool. If two nodes want to communicate with each other, they search for a common key space. To identify the common key space between the neighbors, the sensor node will broadcast the message ID to the neighbors. If two nodes share a common key, then the nodes start communicating each other. If there is no common key space, then the neighboring nodes try to establish a secure communication through intermediate nodes. Eschenauer and Gligor [1] were the first to propose a probabilistic key distribution scheme based on a random graph construction. This scheme is referred as basic scheme. From a key pool of size S, a set of M distinct keys is randomly selected and is assigned to a sensor node. The size of the key pool S and the size of the key ring M are set to ensure that the network is connected and a pair of sensors holds a common key with high probability. The drawback is EG scheme requires large memory to achieve better connectivity.

DDHV scheme [2] combined Blom's scheme [3] and the basic scheme. Each node picks some rows randomly from the available key spaces. Two nodes could communicate with each other if they have rows from at least one common key space. Benefiting from Blom's scheme, the scheme has better resilience against node capture than the basic scheme. Better connectivity is achieved with less number of key spaces. The major disadvantage in the above scheme is that, when the attackers compromise sufficient number of nodes, it is possible to reconstruct the complete key pool. Liu and Ning [4] and Du and others [5] also developed a scheme based on pre-deployment knowledge. The key predistribution is developed based on random subset assignment, and the grid based key predistribution scheme to reduce the fraction of links compromised thereby establishing a secure communication.

Motivated by the fact of insufficient hardware resources, a great deal of research has focused on the cryptography based solutions for lightweight computation but at the similar level of security. Recent progress in implementation of elliptic curve cryptography (ECC) on sensors proves public key cryptography (PKC) is now feasible for resource constrained sensors. ECC provides the same level of security at a very shorter key length when compared with that of the earlier public-key cryptographic technique Rivest Shamir Adleman Algorithm (RSA). Thus, the amount of computational complexity needed to attain greater security is reduced and it can be effectively implemented into tiny nodes with smaller processor and smaller memory size.

In this paper, effort is taken to make use of ECC for predistributing the keys to the sensor nodes. In the proposed scheme, a seed key, which is a distinct point in an elliptic curve, is assigned to each sensor node. The private key ring for each sensor node is generated using the point doubling mathematical operation over the seed key, and the key ring is predistributed into the sensor node prior to deployment. When two nodes share a common private key, then a link is established between these two nodes. The performance is evaluated in terms of connectivity and resilience against node capture.

The paper is organized as follows. In section II, related works are presented. Section III gives an introduction to ECC. Section IV elaborates upon the proposed scheme. Section V gives an evaluation based on connectivity and resilience against node capture. Section VI provides the conclusion and possibilities for future work.

II. Related Works

Perrig and others [6] presented a suite of security building blocks optimized for resource constrained environments and wireless communication. Security protocols for sensor networks (SPINS) have two secure building blocks: SNEP and μTESLA. SNEP provides the following important baseline security primitives: data confidentiality, two-party data authentication, and data freshness. A particularly hard problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks. μTESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments. They implemented the above protocols and showed that they are practical even on minimal hardware: The performance of the protocol suite easily matches the data rate of our network. Additionally, they demonstrate that the suite can be used for building higher-level protocols.

The design proposed by the authors is suitable for all types of networks with low-end devices. The design primitive only depend on the symmetric cryptography and it is applicable to large number of device configurations as indicated earlier. In the scheme proposed by the authors, the energy spent for security is negligible compared to the energy spent for sending or receiving messages and they have identified that it is possible to encrypt and authenticate all sensor readings. The communication costs are also small. In this scheme, it is identified that data freshness, authentication, and confidentiality properties use only 6 bytes out of 30 byte packets. So, it is possible to implement these properties on a per packet basis. If the platform is more powerful, block ciphers like RC5 can be used. SPINS provide very strong resilience with data freshness and point-to-point authentication. It also provides good storage

and communication capabilities.

In [7], Gaubatz and others proved that public key cryptography (PKC) reduces the complexity involved in the implementation of many typical security services and in turn reduces transmission power due to less protocol overhead. In this paper, the authors have presented in depth comparative analysis of three popular public key implementations: Rabin's scheme, Ntru Encrypt/Ntru sign, and ECC. They also described how the fundamental security services such as broadcast authentication, data encryption, node to node key distribution, and addition of new nodes, gets benefited from PKC. Finally, they have concluded that PKC is best suited for constrained environments with the fact that they achieve reduced traffic overhead with less computation cost and considerably fast.

Wander and others [8] have presented a comparison of two public key algorithms, RSA and ECC, based on energy cost analysis considering mutual authentication and key exchange between two trusted parties such as two nodes in a WSN. The experiments were done on an Atmel Atmega low power microcontroller and it was found that PKC is viable in 8-bit energy constrained platforms. Based on the comparative analysis, authors have proved that ECC is advantageous over RSA as it reduces computation time and also the amount of data transmitted and stored.

Li [9] proposed a key distribution scheme based on PKC for WSNs. Here, the scheme does not need to predistribute pair wise keys. A pair wise key is established between two nodes after deployment according to a specific routing algorithm proposed by the author. The scheme guarantees that there is a direct pair wise key between two nodes that need communication frequently which in turn decreases the overhead. To achieve best results, the authors have adopted the two-party key exchange algorithm (TPKE) and hash function. The authors have proved that the proposed scheme provides higher connectivity and at the same time save memory.

Murphy and others [10] have proposed a hardware and software codesign approach to implement public key algorithms on resource constrained node platforms. In this approach, they have successfully mapped a public key cryptosystem based on Rabin's scheme on to the Tyndall motes. They proposed efficient architectures that successfully execute the public key algorithms using minimal resources.

Murphy and others [11] presented an area efficient processor for public key cryptography in WSNs. The processor designed by the authors aims in high scalability and flexibility while using minimal hardware. This type of PKC processor, which uses minimal hardware resources while maintaining high flexibility, is suitable for WSNs. The processor architecture is scalable and all hardware configuration support arbitrary bit lengths and domain parameters. The processor designed by the authors is capable of supporting both RSA and ECC operations using arbitrary security parameters. The authors implemented the architecture in the FPGA layer of the 25 mm Tyndall mote and it can also be incorporated into a microcontroller as instruction set extension. Finally, the authors have concluded that the processor is suitable for constrained platforms such as WSNs.

Pugliese and Santucci [12] have proposed a novel scheme for generation of pair wise network topology authenticated keys in a WSN using vector algebra in GF(q). The two important blocks of the proposed scheme are network topology authentication and hybrid key cryptography. The former means that a cryptographic key can be generated if and only if the current network topology is compliant to the planned network topology, which acts as the authenticated reference. The latter means that the proposed scheme is a combination of features from symmetric (for ciphering and authentication) and asymmetric cryptography (for key generation model). The analysis showed that the proposed scheme is best suited for WSNs in terms of cost, computational time, and memory usage.

Yao [13] has proposed a security architecture based on identity based cryptosystem, but not requiring key hand shaking. The analysis shows that the proposed scheme ensures a good level of security and is very much suitable for the resource constrained environments like WSNs.

Jiang and Liu [14] have proposed a key management scheme based on clustering model. To achieve the best results, the authors have adopted two popular techniques, namely, an identity based authentication mechanism and an elliptic curve cryptosystem to encrypt message and keys. Due to the characteristics of identity based authentication mechanism, there is a possibility of achieving 100% connectivity. The basic idea of the proposed scheme is to introduce two level of security. The first level being elliptic curve cryptosystem, in which even if some nodes are compromised by the adversary, the remainder of the network remains fully secure as it is difficult to break elliptic curve discrete logarithm problem. The second level being, mutual authentication between any two nodes, that implies any node can ascertain the identity of the nodes to which it is communicating. The authors have proved that the proposed scheme is highly secure and can achieve 100% connectivity along with nodes updating mechanism which supports nodes addition and revocation. The authors did not address the issue of changing the cluster head's responsibility among the nodes, which may result in battery exhaust of a node if the same node continues to be a cluster head as it is a power constrained environment. Secondly, if a cluster head is compromised by the adversary, there is a

possibility that the corresponding group may be compromised or may get completely detached from the network.

Szcsechowiak and others [15] have implemented ECC and pairing based cryptography (PBC) on the MICA2 and Tmote Sky nodes. The authors proved that PKC is viable and attractive for power constrained sensor nodes by presenting their updated results on implementing ECC and PBC over two of the most popular WSN platforms as mentioned earlier. The author's work was the first known implementation of pairings over binary field for sensor networks. The authors have analyzed the performance of their ECC and PBC implementation on sensor nodes based on parameters such as computation time, current drawn, energy consumption, and RAM and ROM requirements. As a result of their analysis, the authors have presented two conclusions. First, ECC over prime field is not always the best option as pairings over GF(2^m) seem to be more efficient on MICA2 and Tmote Sky architectures. Second, PBC offers fast pairing computation which enables the use of new ways of achieving security in WSN such as identity based encryption.

Shan and Liu [16] have proposed a method to improve the resilience of the existing random key predistribution scheme. In this approach, hashing of keys in the key pool is performed using one way hash function. If two sensor nodes choose the same key, they derive two different keys by hashing with different hash functions. As a result, whenever a sensor node is captured, no key information will be revealed to the adversary because the one way hash function is not invertible. To analyze the proposed scheme, the authors have adopted two different types of measurements: the number of additional compromised links (ACL) and the average insecurity degree, where ACL measures the resilience against node capture and the second measurement ensures the security of each link key. The main advantage of the proposed scheme lay in that the amount of information revealed is reduced to a greater extent when a sensor node is captured but with an additional memory and computation.

The various schemes discussed in the literature focus on effectively utilizing the PKC architecture to minimize the wireless sensor network's constraints, such as memory usage, computation cost, and energy utilization, while simultaneously providing security. In this paper, a key predistribution scheme is proposed in which point doubling property of ECC is used for generating the key ring and finally the performance is analyzed based on resilience and connectivity. From the analysis, it can be inferred that the driving concept in the proposed scheme is to reduce the number of keys predistributed into the nodes thereby overcome the constraints of the WSNs, such as limited memory, limited computation allowed, limited bandwidth, limited battery power, and, at the same time, achieve maximum connectivity with perfect resilience.

III. Elliptic Curve Cryptography

Two types of public key cryptosystems which have had extensive research for many years are RSA and ECC. Despite being developed as long ago as 1977, RSA remains the most popular public key encryption technique. Koblitz and Miller developed ECC in 1985. Its approach depends on the mathematics of elliptic curves. It was proved that ECC could provide same level of security when compared to RSA but with a smaller key size. For example, a 160-bit ECC key has the same security level as a 1,024-bit RSA and a 224-bit ECC key has the same security level as a 2,048-bit RSA key [8],[17]. An RSA scheme uses key size ranging from 512 bits to 2,048 bits. An RSA scheme takes message M converts it into a cipher text C using the key K. The Chinese remainder theorem can be used to make RSA more efficient in which two large prime numbers p and q are multiplied to get modulus n. With these modular multiplications, the Chinese remainder theorem can reduce the computation time by 75% [17]. Other methods like Montgomery multiplication and optimized squaring are available which can reduce the complexity of RSA by 25% [17].

On the other hand, ECC can be implemented by using point multiplication on elliptic curves over prime integer fields or binary fields [18]. However, in WSN environments, point multiplication on elliptic curves over prime integer fields is preferred because binary fields are not suitable for tiny processors. Operations of ECC scale linearly which makes it more suitable than RSA in processors with small word sizes. Also, the security level increases with the increase in the key size. For comparison purposes, ECC 160, ECC 224, RSA 1,024, and RSA 2,048 were implemented on two 8-bit platforms. ECC outperformed RSA on both the platforms, that is, ECC with a 160-bit key resulted in a private key faster than RSA 1,024, and ECC with 224-bit key resulted in private key faster than RSA 2,048 [17]. Basically, elliptic curves can be defined over real numbers and finite fields. The point doubling property which is used for generation of key pool in the proposed scheme is one of the important properties of elliptic curves over finite fields.

1. Elliptic Curves over Finite Fields

ECC makes use of elliptic curves in which the variables and coefficients are restricted to elements of a finite field. There are two families of elliptic curves defined for use in cryptography [19]: prime curves defined over odd prime field F_p and binary curves defined over Galois field $GF(2^n)$.

The curve of interest is the prime curve because of its easy implementation in software and simplified arithmetic. A finite field F_p, where p is an odd prime number, is defined as a set of all integers between 0 and p–1. The elliptic curves over a finite field are defined by

$$y^2 \bmod p = x^3 + ax + b \bmod p, \quad (1)$$

where the coefficients a and b and the variables x and y all take values only from the finite field. It can be represented as $E_p(a, b)$. A point on the elliptic curve can be represented as $P=(x, y)$, where $x, y \in F_p$. The modulo p function performs a wrapping around operation so that the elements are all within F_p. Thus, the geometric shape of the curve is not preserved whereas its Abelian properties are intact. Elliptic curves over finite fields have various important properties such as additive identity, negation of a point, point addition, point doubling, and point multiplication out of which the proposed scheme is based on point doubling, addition, and multiplication properties.

2. Point Doubling

The double of a point on the curve is also a point on the curve. If P is a point on the elliptic curve, then $2P$ also lies on the curve. This is a specific case of point addition where $Q=P$ and valid for all points in the curve [19]. The arithmetic description of point doubling is as follows. If $P = (x_P, y_P)$ with $P \neq 0$, then $2P=P+P=(x_{2P}, y_{2P})$ is determined by

$$x_{2P} = (\lambda^2 - 2 * x_P) \bmod p, \quad (2)$$

$$y_{2P} = [\lambda(x_P - x_{2P}) - y_P] \bmod p, \quad (3)$$

where

$$\lambda = \left\lfloor (3 * x_P^2 + a) / (2 * y_P) \right\rfloor \bmod p. \quad (4)$$

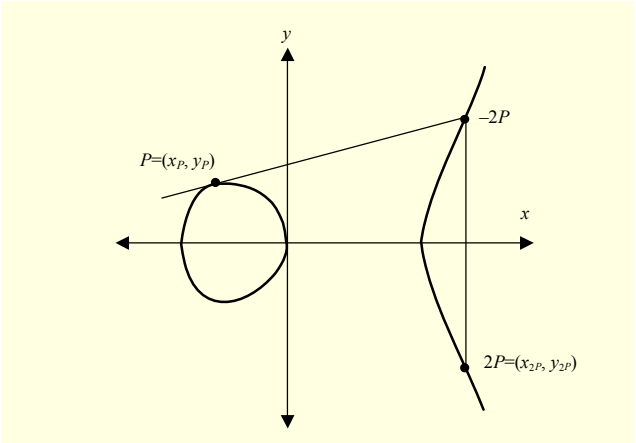

Fig. 1. Point doubling in elliptic curve.

The geometric proof is similar to point addition. If a tangent is drawn to the point P in the curve over real field, the successive point of intersection of the line with the curve is found to be the negation of the doubled point $2P$ as shown in Fig. 1.

IV. Proposed Scheme

The proposed scheme involves key predistribution technique using ECC. A unique seed key, which is an elliptic curve point, is assigned to each node and a private key ring is generated statistically prior to deployment by performing point doubling and addition operations over the seed key. Finally, the key ring is predistributed to the sensor nodes prior to deployment. The properties of elliptic curve are used in the generation of private keys of each node. Link formation between any pair of nodes occurs if they share a common private key. Better connectivity is achieved in this scheme, compared to the already existing schemes. The private key ring for each sensor node is generated using the point addition and doubling mathematical operation over the seed key. When two nodes share a common private key, then a link is established between these two nodes. By suitably choosing the value of the prime field and key ring size, the probability of two nodes sharing the same private key could be increased.

1. Key Management Protocol

The proposed key predistribution scheme consists of three different phases: key generation phase, key predistribution phase, and key agreement phase. In the key generation phase, an appropriate elliptic curve and the corresponding elliptic curve parameters are chosen to generate the elliptic curve points otherwise termed as seed keys in the proposed scheme. In the next phase, each node is assigned a unique seed key with which a key ring is generated by performing point doubling and addition operations over it. The key ring is predistributed into the sensor nodes prior to deployment. After deployment, any two neighboring nodes can form a secured link if they share a common private key. If two neighboring nodes failed to find a common key, the nodes can establish link through an intermediate node with which they share a common key, known as path key establishment. The protocol description is shown in Fig. 2.

The proposed scheme consists of four important stages; namely, elliptic curve parameter selection, generation of seed keys as points of the chosen elliptic curve, generation of the private keys by point multiplication of the seed key prior to node deployment, and link formation between the nodes that share a common private key.

Phase I
(i) Choose elliptic curve and elliptic curve parameters according to dimensions and applications of the sensor network.
(ii) Choose appropriate values of prime field 'p', elliptic curve coefficients a & b.

Phase II
(i) Generate elliptic curve points that satisfy the chosen elliptic curve.
(ii) Each sensor node is allotted a unique key known as seed key.
(iii) Generate a pool of private keys for each node based on seed key.

Phase III
(i) Any two neighboring nodes can form a link if they share at least one common key. If a link is directly formed, it is called link key.
(ii) Otherwise, if the neighboring nodes do not share a common key, they try to establish a path key through an intermediate node.
End

Fig. 2. Protocol description of the proposed scheme.

Table 1. Seed keys for $E_{53}(9, 17)$.

(0, 21)	(0, 32)	(2, 19)	(2, 34)	(4, 8)
(4, 45)	(5, 9)	(5, 44)	(7, 23)	(7, 30)
(10, 10)	(10, 43)	(11, 4)	(11, 49)	(13, 23)
(13, 30)	(14, 5)	(14, 48)	(15, 20)	(15, 33)
(16, 21)	(16, 32)	(23, 25)	(23, 28)	(27, 11)
(27, 42)	(31, 6)	(31, 47)	(32, 1)	(32, 52)
(33, 23)	(33, 30)	(34, 6)	(34, 47)	(37, 21)
(37, 32)	(39, 3)	(39, 50)	(41, 6)	(41, 47)
(43, 26)	(43, 27)	(45, 4)	(45, 49)	(48, 18)
(48, 35)	(50, 4)	(50, 49)	(51, 16)	(51, 37)
(52, 22)	(52, 31)			

2. Elliptic Curve Parameter Selection

Elliptic curve parameters are chosen according to the dimensions and application of the sensor network. The parameter generally consists of the value of the prime field p and the elliptic curve coefficients a and b. For a sensor network comprising of n nodes, the value of p is a prime number larger than n. For example, for a sensor network of 50 nodes, the optimum value of p is 53. In this, the values of a and b are chosen as 9 and 17, respectively.

3. Generation of Seed Keys

For a sensor network of 50 nodes, the value of the prime number is assumed to be 53 which is the next largest prime to 50 as mentioned earlier. If this condition is satisfied, exactly 52 elliptic curve points (seed keys) will be generated as shown in Table 1. Each node is then assigned with a unique seed key, over which point addition and doubling process is performed to generate a key ring.

Table 2. Key rings for $P(0, 21)$ & $P(27, 11)$.

1P	(0, 21)	(27, 11)
2P	(16, 21)	(14, 5)
3P	(37, 32)	(5, 44)
4P	(32, 1)	(10, 43)
5P	(4, 8)	(41, 6)
6P	(43, 26)	(0, 21)
7P	(50, 4)	(16, 21)
8P	(41, 47)	(23, 28)
9P	(27, 11)	(31, 6)
10P	(2, 19)	(33, 23)

4. Private Key Pool Generation

A key ring of private keys is generated for each sensor node prior to deployment and it is predistributed into the node's memory. The point multiplication mathematical operation is used in this stage. For every seed key P, its scalar multiples $2P$, $3P$,..., rP are generated, where r is an integer. The parameter r indicates the number of times point multiplication operation performed and is termed as the private key-ring size. Thus, for example, a seed key of node 1 $P(0, 21)$ and node 2 $P(27, 11)$ generates its ten private keys as shown in Table 2 by using the expressions (2), (3), and (4), respectively.

Example. The elliptic curve for the above mentioned assumptions is given by

$$y^2 = x^3 + 9x + 17, \tag{5}$$

where $a = 9$ and $b = 17$ are chosen based on the following condition mentioned in [19]:

$$4a^3 + 27b^2 \neq 0. \tag{6}$$

For example, if a network of 50 nodes is considered for the analysis, then the value of the prime number 'p' is assumed to be 53, which is the next largest prime to 50, so that 52 elliptic curve points can be generated which satisfies (5), and each node can be assigned a unique seed key which is nothing but an elliptic curve point as shown in Table 1.

Suppose a seed key is randomly assigned to a node from Table 1, for example, $P(0, 21)$. Then, the private key ring can be generated with the following steps using (2) through (4):

$$2P = P + P$$
$$\lambda = [9/42] \bmod 53$$
$$\therefore \lambda = 57$$
$$x_{2P} = [57^2 - 2(0)] \bmod 53 = 16$$
$$y_{2P} = [57(0-16) - 21] \bmod 53 = 21$$
$$2P = (16, 21)$$

In the above mentioned case, that is, for $2P=P+P$, both the points are equal points. However, for $3P=2P+1P$, the points involved are different. In this case, the private key is computed using the following expressions [18]:

$$\lambda = \left[y_Q - y_P / x_Q - x_P \right] \bmod p\,, \tag{7}$$

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p\,, \tag{8}$$

$$y_R = [\lambda(x_P - x_R) - y_P] \bmod p\,, \tag{9}$$

Likewise, the other points in the key ring can be generated as shown in Table 2.

5. Link Formation

Each sensor node is predistributed with its corresponding private key ring. When two nodes share at least one common private key, they form a link. Since r private keys (key ring size) per sensor node are generated and the total number of points in the elliptic curve approximately being p, the probability of two nodes to share a common key is obtained by

$$P' = 1 - P'', \tag{10}$$

$$P'' = (p-r)\times(p-r-1)\times(p-r-2)\times\cdots \times(p-r-r)/[(p-2\times r)!\times p^r], \tag{11}$$

$$P'' = (p-r)!/[(p-2\times r)!\times p^r]. \tag{12}$$

Therefore, from (10) and (12), we get

$$P' = 1 - \{(p-r)!/[(p-2\times r)!\times p^r]\}, \tag{13}$$

where p is the key pool size, r is the key ring size, P' is the probability of two nodes sharing a common key, and P'' is the probability that two nodes do not share a key. Thus, the probability of common private key overlap and therefore number of links can be increased by increasing the parameter r. By this process, the network gets connected.

V. Simulation Results and Discussion

The proposed scheme is analyzed by simulating it in a WSN in the presence of various attacks such as random, brute force, and Sybil attacks. First, a WSN comprising of 100 sensor nodes deployed randomly in a 50×50 m^2 area is simulated. Then, malicious nodes are introduced into the network. The performance of the network under the influence of these malicious nodes is analyzed in terms of connectivity and resilience analysis. Connectivity analysis gives the relationship between the probability of two nodes sharing at least one key space and the varying key ring size. It explains the network connectivity and link formation among the nodes. The resilience analysis shows the probability of the network getting captured with increasing number of malicious nodes. A comparative analysis is done between the proposed scheme and the network formed by Blom's method of symmetric key generation. The reason for choosing Blom's scheme for comparison is that our proposed protocol is also a straight forward method for key predistribution like Blom's method, without considering the factors like deployment knowledge, clustering, cluster reformation, and key manipulation. If these factors are considered, then comparison can be made with other key management protocols. In the case of Blom's scheme, if a node is compromised by the adversary, it will come to know about the row of private matrix A and column of public matrix G, and the adversary may succeed in spreading the attack in a faster manner by exchanging the columns of G with the neighbor nodes and computing the pair wise keys. However, in the proposed protocol, the adversary cannot succeed in spreading the threat in a faster manner because the key generation conducted offline is purely based on the values of elliptic curve parameters like the prime field 'p', the elliptic curve, and the elliptic curve coefficients a and b. This difference can be noticed in the comparative resilience analysis curve.

1. Connectivity Analysis

Connectivity graph depicts the relationship between the probability of two nodes sharing a private key and the key ring size. Figure 3 show the WSN formed using the Blom's scheme with some number of malicious nodes introduced in it whereas Fig. 4 shows the WSN formed by using the proposed scheme. On comparing Figs. 3 and 4, it can be inferred that connectivity among the nodes is good in the case of proposed scheme.

Figure 5 depicts the connectivity graph of the proposed scheme. It is inferred from Fig. 5 that as the key ring size is increased, the probability of link formation also gets increased. Thus, an optimum value of key ring size can be chosen corresponding to the required probability of link formation for a given sensor network density. It is observed that, for a given key ring size, as the size of the key pool decreases, the probability of link formation increases. Hence, it is essential to choose optimum sizes of key pool and key ring. It is also

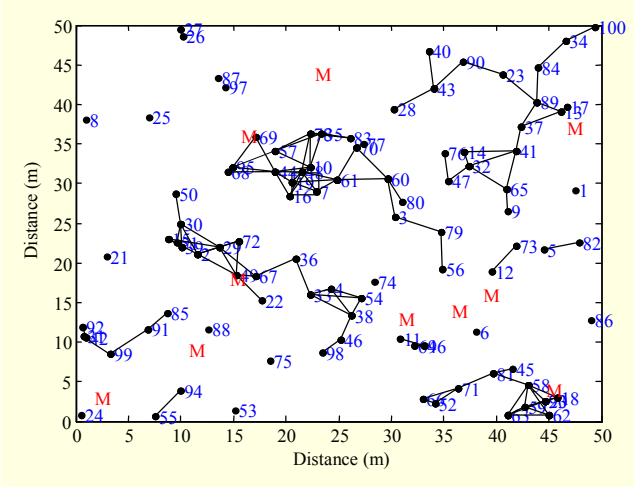

Fig. 3. WSN formation with Blom's scheme.

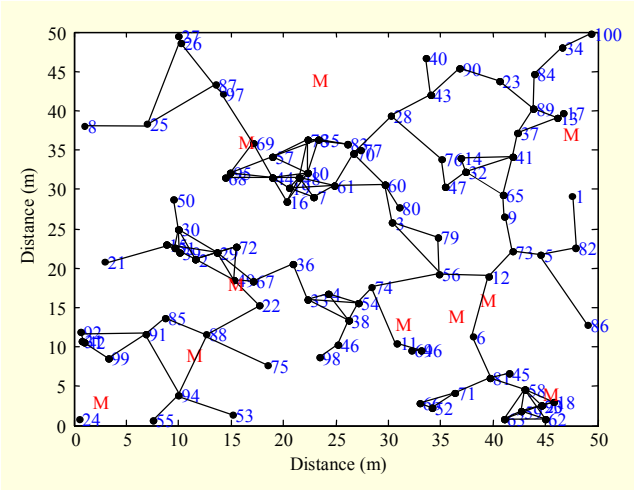

Fig. 4. WSN formation with proposed scheme.

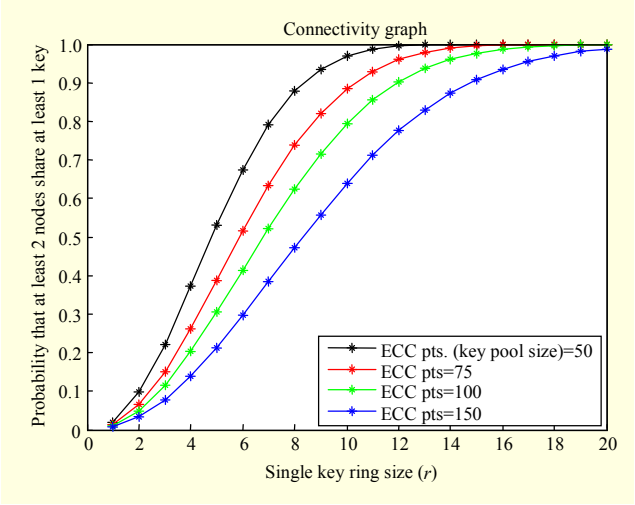

Fig. 5. Connectivity analysis of the proposed scheme.

inferred from Table 2 that even though the seed keys are assigned randomly to the nodes, at least two to three private keys are in common and hence 100% connectivity can be achieved similar to the scheme proposed by Jiang and Liu [14]. The advantage of the proposed scheme is that the same level of connectivity is achieved with single level of security and less number of keys. Hence, the memory requirement and computation complexity is less in the proposed scheme when compared to the idea proposed in [14].

The WSN formed using the proposed scheme has higher connectivity compared to the network formed with the Blom's scheme. The analysis also shows that we need to choose optimum sizes of key pool and key ring to achieve required connectivity in the network. From Fig. 4, it is inferred that the network is almost fully connected when compared to Fig. 3, and Fig. 5 infers that the maximum connectivity is achieved when the key ring size reaches 10 and above, as depicted analytically in Table 2.

2. Resilience Analysis

Resilience analysis gives the relationship between the number of malicious nodes introduced into the network and the probability of the complete network getting captured. A set of malicious nodes are randomly introduced in the network and checked for how far the attacker could be successful in capturing the entire network for a trial of fifty runs. Different numbers of malicious nodes are set to run the simulation, and the number of times the network is captured is recorded under three different attacks as mentioned earlier. Finally, a comparative analysis is done between the resilience curve of the proposed scheme and Blom's scheme.

Figure 6 shows the comparative resilience analysis between Blom's scheme and the proposed scheme for different types of attacks, namely Sybil, brute force, and random attacks, with the size of the network being 100. It is inferred that the network is least resilient in the case of Blom's scheme as it is compromised for larger number of times with least number of malicious nodes introduced into the network. It is also inferred that, in the proposed scheme, the network gets compromised completely, only with more number of malicious nodes introduced when compared to the performance of the basic scheme thus clearly out performs the existing schemes and hence highly resilient. For example, from Fig. 6, it is inferred that under a Sybil attack, the network formed with Blom's symmetric key generation gets compromised completely when only 5 malicious nodes are introduced into the network, whereas, with the proposed scheme, the complete network gets compromised when the malicious nodes count increases to 24 and hence highly resilient.

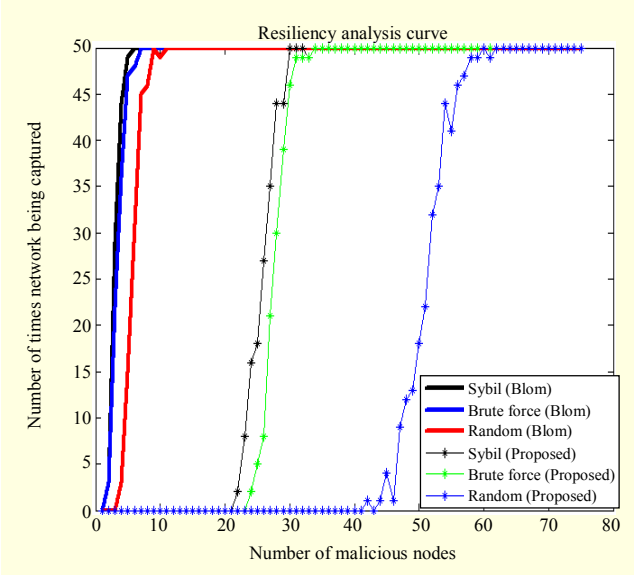

Fig. 6. Comparative resilience analysis (n=100).

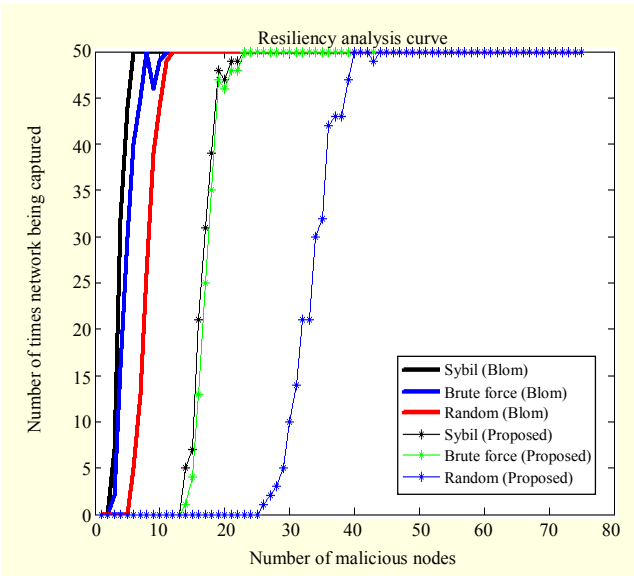

Fig. 7. Comparative resilience analysis (n=75).

Figures 7 and 8 show the comparative resilience analysis for a network size of 75 and 50, respectively. From the figures, it can be inferred that the proposed scheme out performs the existing schemes as the number of malicious nodes required to compromise the entire network is more when compared with the Blom's scheme in which the network gets compromised with less number of malicious nodes introduced.

3. Energy and Complexity Analysis

In the proposed scheme, each node is assigned a seed key, which is nothing but an elliptic curve point. Before deployment,

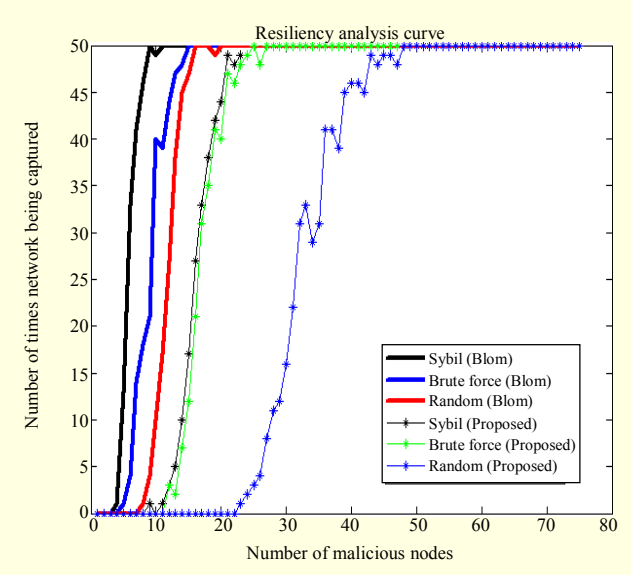

Fig. 8. Comparative resilience analysis (n=50).

point multiplication and point doubling properties of ECC are used to generate keys in the key ring. After deployment, the neighboring nodes form secured links if they share at least one common key. From the analysis, it is inferred that it is sufficient to generate a maximum of ten keys to achieve very high connectivity. The same is the case for the addition of new nodes. As mentioned in the literature, ECC can achieve the same security level with shorter key size when compared to other PKC, which requires a larger key size. For example, RSA requires a key size of 1,024 bits to achieve sufficient security, whereas ECC can achieve the same security level with only 160-bit key size. Consequently, the power and memory requirement gets reduced many folds in the proposed scheme.

In addition to this, because the key size is shorter, the bandwidth requirement is also less when compared to the other public key cryptosystems. As a result, the complexity in terms of computation of the proposed scheme is less. Parameter selection and algorithm implementation is simple in the proposed scheme, while also achieving a better security level compared to the existing schemes.

VI. Conclusion

In this paper, we proposed a novel approach to attain efficient and secure key-predistribution technique using the ECC in a WSN. The particular parameters for elliptic curve were chosen, and the corresponding elliptic curve points were calculated. A distinct seed key is assigned to each sensor node from these elliptic curve points. The point doubling mathematical operation is used to generate private key ring for each sensor node and predistributed into it prior to deployment.

Since the number of elliptic curve points is almost in the range of the prime field value p, such a prime value p that is greater than the number of sensor nodes in the network is used. Thus, two sensor nodes form a link if they share at least one common private key. Finally, the resistances of our model to various sensor network attacks, such as brute force, Sybil, and random attacks, were shown with the help of simulation results. The simulation results shows that the proposed model has better resistance to network attacks and requires less memory to achieve better connectivity and resilience when compared to Blom's scheme.

References

[1] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conf. Comput. Comm. Security*, 2002, pp. 41-47.

[2] W. Du et al., "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," *Proc. 10th ACM Conf. Comput. Comm. Security*, 2003, pp. 42-51.

[3] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," *Adv. Cryptology: Proc. EUROCRYPT'84*, 1985, pp. 335-338.

[4] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *Proc. 10th ACM Conf. Comput. Comm. Security*, 2003, pp. 52-61.

[5] W. Du et al., "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," *Proc. IEEE INFOCOM*, 2004, pp. 586-597.

[6] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," *Proc. Wireless Netw.*, vol. 8, Sept. 2002, pp. 521-534.

[7] G. Gaubatz et al., "State of the Art in Ultra-low Power Public Key Cryptography for Wireless Sensor Networks," *Proc. Third IEEE Int. Conf. Pervasive Comput. Commun. Workshops, PerCom Workshops*, 2005, pp. 146-150.

[8] A.S. Wander et al., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. Workshops, PerCom Workshops*, *2005,* pp. 324-328.

[9] X. Li et al., "A Key Distribution Scheme Based on Public Key Cryptography for Wireless Sensor Networks," *Proc. Int. Conf. Computational Intelli. Security, ICCIAS*, 2006, pp. 1113-1116.

[10] G. Murphy et al., "Hardware-Software Implementation of Public-Key Cryptography for Wireless Sensor Networks," *Proc. Irish Signals Syst. Conf.*, Dublin, Ireland, 2006, pp. 463-468.

[11] G.D. Murphy, E.M. Popovici, and W.P. Marnane, "Area-Efficient Processor for Public-Key Cryptography in Wireless Sensor Networks," *Proc. 2nd Int. Conf. Sensor Technol. Appl.*, 2008, pp. 667-672.

[12] M. Pugliese and F. Santucci, "Pair-Wise Network Topology Authenticated Hybrid Cryptographic Keys for Wireless Sensor Networks Using Vector Algebra," *Proc. 5th IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, 2008, pp. 853-859.

[13] J. Yao, "A Security Architecture for Wireless Sensor Networks Based-On Public Key Cryptography," *Proc. Int. Conf. Wireless Comm. Networking Mobile Comput.*, 2009, pp. 1-3.

[14] J.W. Jiang and J.H. Liu, "Research on Key Management Scheme for WSN Based on Elliptic Curve Cryptosystem," *Proc. 1st Int. Conf. Networked Digital Technol.*, 2009, pp. 536-540.

[15] P. Szczechowiak et al., "NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks," *Lect. Notes Comput. Sci.*, vol. 4913, 2008, pp. 305-320.

[16] T.H. Shan and C.M. Liu, "Enhancing the Key Pre-distribution Scheme on Wireless Sensor Networks," *Proc. Asia-Pacific Services Comput. Conf.*, 2008, pp. 1127-1131.

[17] N. Gura et al., "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," *Proc. 6th Int. Workshop Cryptographic Hardware Embedded Syst.*, Boston, Mass., vol. 3156. Aug. 2004, pp. 925-943.

[18] D. Malan, M. Welsh, and M.D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography," *Proc. 1st IEEE Int. Conf. Commun. Netw.*, Santa Clara, CA, Oct. 2004.

[19] William Stallings, *Cryptography and Network Security: Principles and Practice*, 3rd ed., New York: Prentice Hall, 2002.

Kishore Rajendiran graduated with a BE in electronics and communication engineering from Madras University in 1998. He obtained his MTech in communication systems from Pondicherry Engineering College, Pondicherry University, Pondicherry, India, 2003. At present, he is working as an assistant professor in the Department of ECE, Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, Chennai, Tamilnadu, India. Presently, he is working toward a PhD in Anna University, Chennai, India. His current area of research is security issues in wireless sensor networks.

Radha Sankararajan graduated with a BE in electronics and communication engineering from Madurai Kamraj University, India, in 1989. She obtained her ME in applied electronics from Government College of Technology, Coimbatore, India, and her PhD in the area of mobile ad hoc networks from Anna University, Chennai, India. At present, she is working as professor and head of the Department of ECE, Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, India. She has had 33 papers published in international and national journals and conferences. Her current areas of research are security and architecture issues of mobile ad hoc

networks and sensor networks. She received the IETE-S.K. Mitra Memorial Award in October 2006 for the Best Research Paper published in the IETE Journal of Research and the CTS–SSN Best Faculty Award–2007 and 2009 for the outstanding performance for the academic year 2006-07 and 2008-09.

Ramasamy Palaniappan received his BE in electronics and communication engineering from Sri Sivasubramaniya Nadar College of Engineering, Chennai, India. He is presently working for the Indian Space Research Organization. His fields of interest include digital communication, wireless sensor networks, and antennas and RF systems.