Secure Routing in Wireless Sensor Networks using Identity-based Cryptography

Harsh Kupwade Patil
Department of Computer Science
Lyle School of Engineering
Southern Methodist University
Dallas, Texas, USA

Joseph Camp
Department of Electrical Engineering
Lyle School of Engineering
Southern Methodist University
Dallas, Texas, USA

Stephen A. Szygenda
Department of Computer Science
Lyle School of Engineering
Southern Methodist University
Dallas, Texas, USA

Abstract

Wireless Sensor Networks (WSN) have played a crucial role in many military and civilian applications. However, with the increase in popularity of such networks, the demand for security is also increasing proportionally. The new sophisticated attacks can easily compromise these resource constraint networks such as WSN. In this paper, we propose a location and energy efficient routing scheme using identity bases cryptography. We review the classical selective forwarding attack on WSN and see how an identity-based cryptographic scheme using a cross-layer design approach is helpful in circumventing such an attack. In addition, we show that an identity-based cryptographic approach to routing in WSN is more pragmatic then the traditional public key infrastructure (PKI) based schemes.

1 Introduction

Wireless Sensor Networks (WSN) have gained attention in the past decade due to their direct applicability in diverse sectors such as military, health care, habitat and wild life monitoring, industrial process control, home automation and many other applications. A typical sensor network consists of sensor nodes that have a lower storage capacity, processing power, battery levels and communication bandwidth when compared to other ad-hoc networks such as Mobile Ad-hoc Networks (MANET) [1]. Figure 1.1 shows a WSN architecture divided into small clusters. Each cluster has a cluster head, which is responsible for congregating data sent from the nodes within its cluster. It may pre-process data before forwarding it to the sink node.

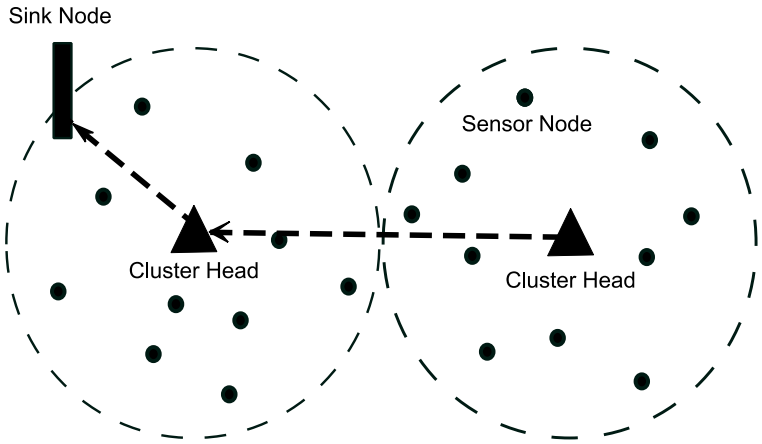

Figure 1.1: Wireless Sensor Network Architecture

The architecture of WSN is usually application-dependent. For example, sensor applications in a processing plant could have a centralized architecture, wherein all the nodes in the network would forward their sensed data to their respective base stations (sink node or a cluster node). On the contrary, in a battlefield environment, nodes may well be distributed in a completely decentralized manner. In such scenarios, each node will have to process data as well as make independent routing decisions. Furthermore, a fusion of the centralized and decentralized architectures could be used in applications where ordinary nodes could act as base stations depending on their energy levels.

Among the many tasks performed by WSN, routing protocols are especially important as they help in data aggregation. However, with the increase in popularity of such networks, the attacks have also increased proportionally [2]. Hence, the need for applying security in routing protocols became evident as the attacks evolved [3]. The new attack vectors not only exploited vulnerabilities in each protocol layer, but also looked for vulnerabilities between layers [4], [5]. Hence, there is a need for designing new security solutions that consider horizontal and vertical layers in providing a holistic solution. In this paper, we propose a new approach to secure routing in WSN by applying identity-based cryptography using a cross-layer design approach, while taking location and energy levels of sensor nodes into consideration.

1.1 Related Work

1.1.1 Routing protocols in WSN

Routing in ad-hoc networks has been very challenging due to node mobility. Hence, a routing path established in the beginning between the source and the destination, may not exist at a later time interval. Furthermore, in a resource constraint environment such as WSN, the energy levels of the intermediate nodes must be considered in making routing decisions.

Routing protocols in WSN can be broadly classified into proactive, reactive, hybrid and location-aware routing protocols [6]. In a proactive routing scheme, each node maintains an up-

to-date routing table by frequently querying its immediate neighbors for routing information. An example of such a scheme is Destination Sequenced Distance Vector (DSDV) routing protocol [7] . However, one of the major drawbacks with such schemes is with the additional overhead due to frequent routing updates. In contrast, reactive routing involves on-the-fly route establishment and is demand driven. It is based on a request-response model. The initial discovery phase to find the destined node could involve flooding and the response phase establishes the transient active routing path. Examples include Ad-hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) [8], [9]. While, hybrid protocol uses the node discovery method of the pro-active routing protocol along with the on-the-fly routing path establishment method to produce a hybrid version of the protocol. Zone Routing Protocol (ZRP) is an example of such a hybrid scheme [10]. In position-aware routing protocols, the nodes select the geographically closest neighboring node when making routing decisions. An example of such a protocol is Geographic and Energy Aware Routing (GEAR) protocol [11]. However, GEAR does not take security into consideration. Most of the security schemes in WSN have focused on symmetric-key cryptography due to the notion that asymmetric-key cryptography (RSA based algorithms) was computationally intensive. However, symmetric-key cryptography has major drawbacks with regard to key management and the security is based upon pre-shared secret keys. With the successful implementation of pairing-based cryptographic algorithms in WSN, a new platform is provided to implement asymmetric-key cryptographic schemes in WSN [12].

1.2 Selective forwarding attack in WSN

Many routing protocols in WSN use a breadth-first spanning tree algorithm to broadcast routing updates [3], [13]. The sink node periodically broadcasts updated routing information to its immediate cluster heads. Then, these cluster heads re-broadcast this information to their immediate neighbors, and the process continues recursively. During this process, each intermediate node makes a note of its parent node where the parent node is the first node that was able to make contact with its subordinate node and relay the routing information. When all the active nodes are operational, they should send all the sensed data to their parent node. However, this protocol is vulnerable to many attacks. For example, a simple impersonation attack leading to a sinkhole attack, could totally compromise the entire network (Figure 1.2)

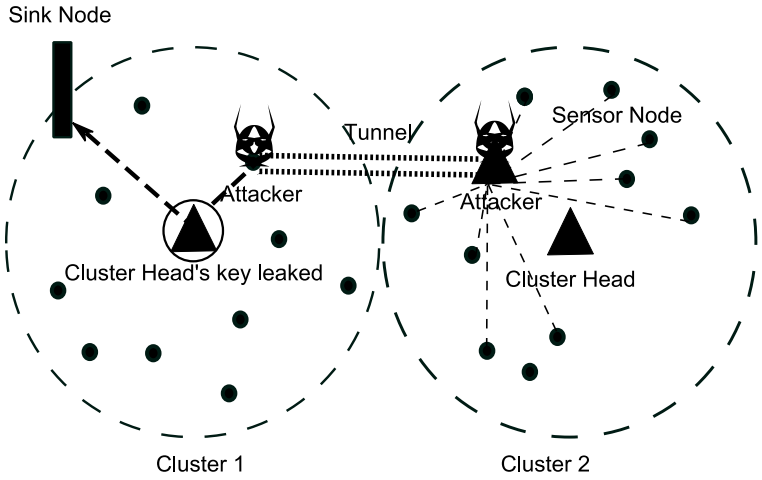

Figure 1.2: Selective forwarding attack in WSN

In the traditional PKI-based architecture, the compromised cluster head in cluster 1, immediately informs about its revoked key to all its immediate neighbors. Let us consider the case where a rogue sensor node is one of its immediate neighbors and is a resource abundant device. This rogue sensor node in cluster 1 will tunnel the revoked key information to its colluder in cluster 2, even before the compromised cluster head in cluster 1 informs its peer in the other cluster. Now, the resource abundant adversary in cluster 2 can impersonate the cluster head in cluster 1 and generate a new public-key as it is aware of the compromised private key. It can re-authenticate to the cluster head in cluster 2 and all the sensor nodes in cluster 2. After proving its authenticity, it can launch a selective forwarding attack, eavesdropping attack and black-hole attack. In addition, the attacker can also launch a route suppression attack by advertising higher energy levels then its compatriots and attract all the data.

2 Identity based cryptography

In 1984, Shamir introduced the concept of using identity as a public key in asymmetric key cryptography [14]. The identity could be any public parameter such as email address, Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) or even an identity assigned by a sensor node's manufacturer. Hence, this new paradigm of cryptography significantly reduces the design complexity because it extirpates the use of public key certificates, which would consume extra storage space and processing power; simplifies revocation process in a decentralized architecture such as WSN; reduces the complexity in verification of digital signatures in a hierarchical system and provides a simpler model for key management.

While, Shamir was able to construct an identity based signature scheme using the RSA algorithm, he was unable to formulate an encryption algorithm, which was an unsolved problem for almost a decade. In 2001, Boneh and Franklin were able to construct an encryption scheme with the help of Weil pairing [15]. At the same time, Cocks proposed a solution using the concept of quadratic residues. This new paradigm of pairing based cryptography led to a flurry of identity based signature/signcryption and key distribution schemes.

The usual trust model of an IBC scheme uses a private key generator (PKG) instead of a certificate authority. Figure 2.1 shows the general method of key distribution in IBC. A PKG is responsible for distributing private keys to its end users.

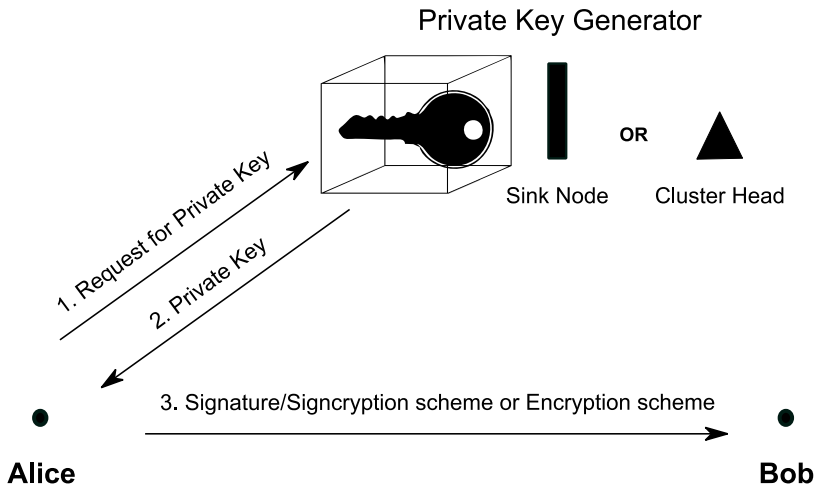

Figure 2.1: Key distribution in Identity-based cryptography

Secure key distribution is achieved using Byoungcheon Lee et al's algorithm [16] , while the problem of key escrow can be solved using the concept of threshold key cryptography (Figure 2.2).

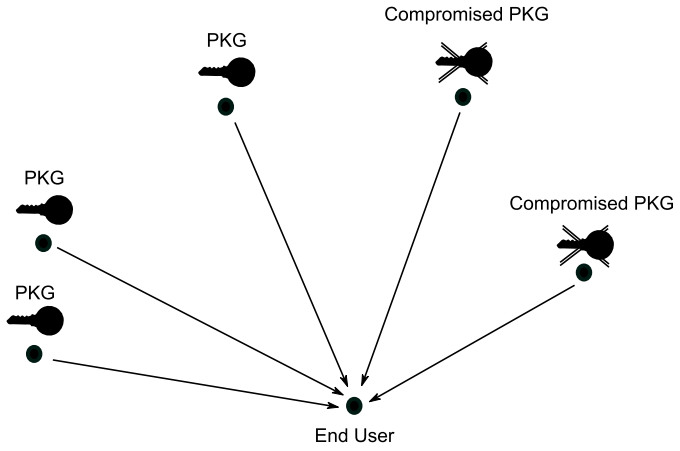

Figure 2.2: Threshold key cryptography

In this scheme, the secret is equally divided among n nodes such if n-1 nodes are compromised, the secret is still not compromised. On receiving the private key corresponding to their identities, the end users authenticate using Hess's algorithm. In addition, they could send signcrypted messages using Lynn's algorithm. Session keys could be produced using Sakai et. al's key sharing algorithm.

2.1 Preliminaries

Let G_1 be an additive group (point subgroup on an elliptic curve over a finite field) and G_2 be a multiplicative group (subgroup of a cyclic group of a larger finite field). Let H_1, H_2 and H_3 be hash functions such that

$$H_1 : \{0,1\}^l \rightarrow G_1 \tag{1.1}$$

where l is the length of the plaintext. Let

$$H_2 : \{0,1\}^l \times G_2 \rightarrow Z_q \tag{1.2}$$

where $Z_q = Z / qZ$. Let $H_3 : G_2 \rightarrow Z_q^*$ and let a bilinear map e exists such that

$$e : G_1 \times G_1 \rightarrow G_2 \tag{1.3}$$

and satisfying the bilinear property. Let $s_0 \in Z_q^*$ be the master secret chosen by the PKG. Then, the master public parameter be

$$P_0 = s_0 P \tag{1.4}$$

where $P \in G_1$. In addition, let $P_1 \in G_1$. Let the message $m \in \{0,1\}^*$.

Let Alice have an identity ID_A, then the private key provided to Alice by the PKG is

$$d_{ID_A} = s_0 H_1(ID_A) \tag{1.5}$$

2.2 Hess's algorithm [17]

In this algorithm, Alice would pick a secret $k \in Z_q^*$, and compute

$$r = e(P_1, P)^k \tag{1.6}$$

She would then compute

$$v = H_2(m, r) \tag{1.7}$$

and

$$u = v d_{ID_A} + k P_1 \tag{1.8}$$

Bob would compute r from (u, v) as shown below:

$$r = e(u, P).e(H_1(ID_A), -P_0)^v \tag{1.9}$$

and then verify the signature as shown below

$$v \stackrel{?}{=} H_2(m,r) \tag{1.10}$$

Figure 2.3 summarizes Hess's algorithm.

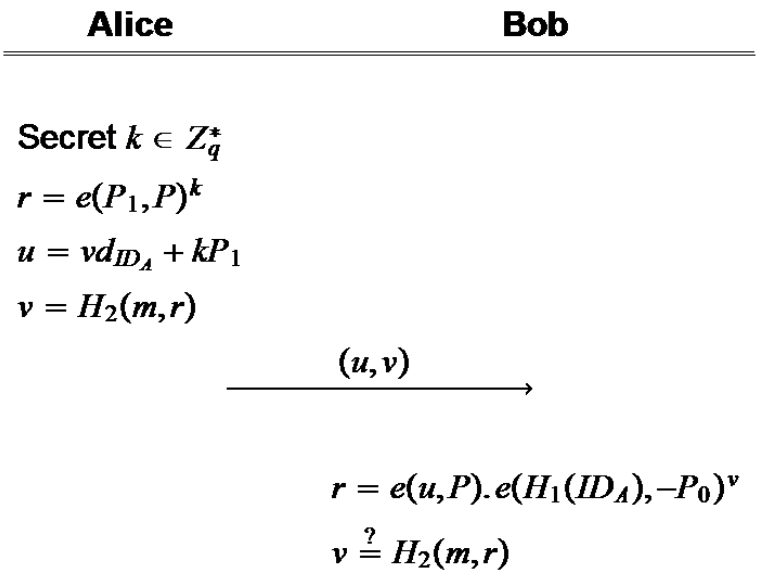

Figure 2.3: Hess's identity based signature algorithm

2.3 Lynn's algorithm [18]

Let

$$H_4 : \{0,1\}^* \times \{0,1\}^* \to Z_q \tag{1.11}$$

$$H_5 : Z_q \times G_2 \to \{0,1\}^* \tag{1.12}$$

and

$$H_6 : \{0,1\}^l \to \{0,1\}^* \tag{1.13}$$

Let $Q_{ID_A} = H_1(ID_A)$ and $Q_{ID_B} = H_1(ID_B)$

In this algorithm, Alice would pick a secret k and compute

$$U = q = H_4(k,m) \tag{1.14}$$

and

$$w = e(d_{ID_A}, Q_{ID_B}) \tag{1.15}$$

The cluster heads or sink nodes can use AES algorithm to encrypt the message (q, w),

$$V = E_{n_{H_5[q,w]}}(k) \tag{1.16}$$

and

$$W = E_{n_{H_6[k]}}(m) \tag{1.17}$$

While the sensor nodes can use Boneh and Franklin's ID based encryption algorithm (explained in Section 2.4). Alice would then send the signcrypted message (U,V,W) to Bob. Bob would use his private key d_{ID_B} and Alice's public key to generate w. He would then retrieve k and m as shown below:

$$Dn_{H_5[U,w]}(V) = k \tag{1.18}$$

$$Dn_{H_{6[k]}}(W) = m \tag{1.19}$$

Figure 2.4 summarizes Lynn's algorithm.

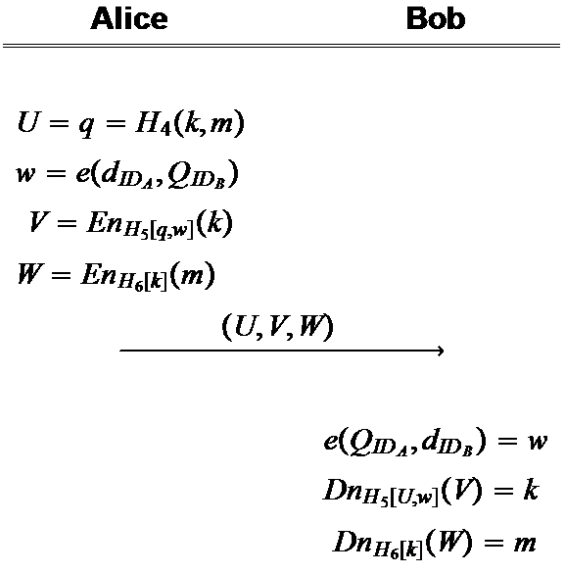

Figure 2.4: Lynn's identity based signcryption algorithm

2.4 Boneh and Franklin's algorithm [15]

Let

$$H_7 : G_2 \rightarrow \{0,1\}^n \tag{1.20}$$

Let Alice pick a secret $k \in Z_q^*$ and compute

$$x_{ID} = e(Q_{ID_B}, P_0) \in G_2 \tag{1.21}$$

She would then compute

$$X = kP \tag{1.22}$$

and

$$Y = M \oplus H_7(x_{ID})^k \tag{1.23}$$

and send the encrypted message $C = (X, Y)$.

Bob would decrypt the message M as shown below

$$Y \oplus H_7(e(d_{ID_A}, X) = M \tag{1.24}$$

Figure 2.5: Boneh and Franklin's identity based encryption algorithm

2.5 Sakai, Ohgishi and Kasahara algorithm [19]

This is a non-interactive key sharing scheme where Alice would use her private key (d_{ID_A}) and Bob's public key (Q_{ID_B}) in generating a session key (Figure 2.6).

$$V = e(d_{ID_A}, Q_{ID_B}) = e(d_{ID_B}, Q_{ID_A}) = e(Q_{ID_A}, Q_{ID_B})^{s_0} \tag{1.25}$$

Alice	**Bob**
$V = e(d_{ID_A}, Q_{ID_B})$	$V = e(d_{ID_B}, Q_{ID_A})$

Figure 2.6: Sakai, Ohgishi and Kasahara identity based key sharing algorithm

2.6 Location and energy aware routing using Identity-based Cryptography

We propose a location and energy-aware routing scheme using identity-based cryptography against the selective forwarding attack discussed in Section 1.2. In this approach :

- Sensor nodes would verify the location information of the cluster head using the triangulation method.
- The nodes will then encrypt data using the cluster head's ID concatenated with the location coordinates. Hence, they are forcing the cluster head to authenticate itself to the sink node with the new location coordinates and obtain the private key. If the cluster head is a rogue entity, it will not be able to authenticate itself to the sink node.
- The cluster head should also prove its authenticity by sending a digital signature with its new identity (ID + Location information). We propose that the cluster heads should also include their power levels in the digital signature, so that sensor nodes are aware of energy levels of their clusters. This attack would also prevent route suppression attack
- The sensor nodes could use Lynn's signcryption scheme of Boneh and Franklin's encryption scheme. Authentication is realized using Hess's algorithm. Ephemeral session keys can be generated using Sakai, Ohgishi and Kasahara algorithm

3 Cross Layer Approach

To combat cross-layer attacks, a cross-layer design approach to routing in essential. With the help of identity-based cryptography, the conventional hop-by-hop routing can be by-passed to overcome sinkhole attacks. Hence, intermediate nodes can simply use IDs of distant nodes and encrypt messages. In traditional PKI based schemes, such techniques could not have been possible, as an intermediate malicious node would never forward its neighbors public key certificates. However, the non-interactive approach helps sensor nodes to send messages to any other node as long as they are aware of their IDs. Furthermore, authentication should not be restricted to application layer, and we propose MAC and Network layer authentication schemes [4]. Cross layer design schemes for key distribution should be considered to facilitate secure key exchange [5].

4 Experimental Results

4.1 TinyPBC cryptographic library

We show that sensor nodes are capable of computing elliptic curve arithmetic proficiently by using Tinypbc library [12]. This library provides suitable pairing operations (Tate pairing) in a sensor node. We use binary elliptic curves over prime curves; as they offer significant computational advantages in a resource constraint environment such as WSN. The platform used for conducting the experiments was on MICA2 Mote, which has an ATmega128 8-bit processor, 128 KB EEPROM chip and a 4KB RAM chip. We make adept implementation of squaring, modular reduction, multiplication and inversion in $F_{2^{163}}$ (NIST irreducible polynomial for the finite field $f(z) = z^{163} + z^7 + z^6 + z^3 + 1$ and $F_{2^{233}}$. Point multiplication is implemented on generic binary curves and Koblitz curves.

4.2 ASSERT

ASSERT is an emulator that emulates node mobility and link interference. Using controlled attenuation, it creates virtual distances. We implement the mesh and star topology to test secure ID based routing schemes.

An ad-hoc resource constraint environment is emulated by creating a topology with 5 sensor nodes in ASSERT. The nodes (v_0,v_1,v_2,v_3 and v_4) are actual MICA2 motes (Figure 4.1).

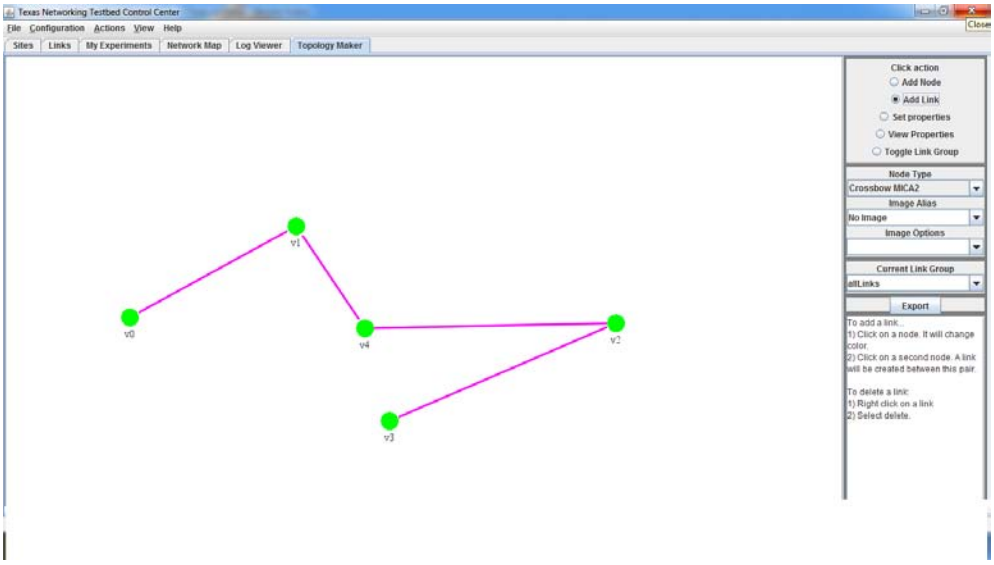

Figure 4.1: Topology creation in ASSERT

Figure 4.2 shows the successful compilation of Sakai et. al's Identity based key agreement protocol in ASSERT. Similarly, algorithms in Section 2 were implemented using TinyPBC and tested on ASSERT.

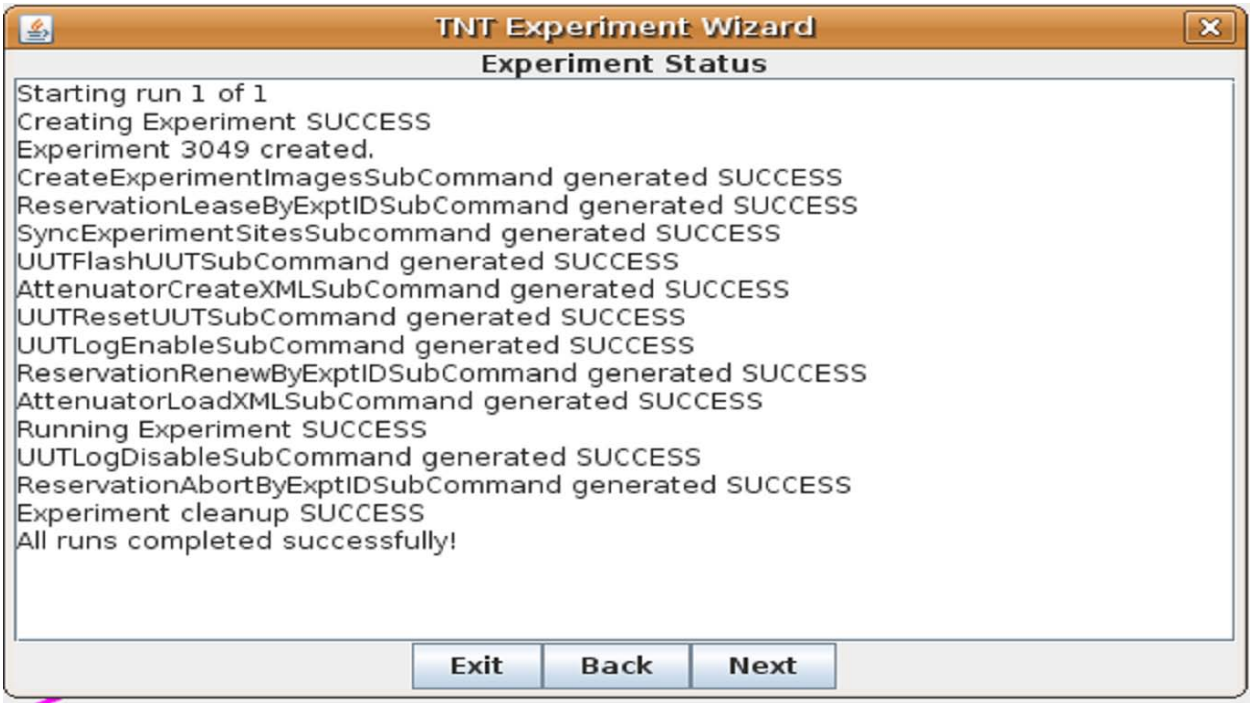

Figure 4.2: Experimental Wizard in ASSERT

We then verified if Sakai et. al's Identity based key agreement protocol can be computed under 0.40 seconds at 163 bit level of security. Consequently, an ID based digital signature can be computed in 2.17 seconds at 233 bit level of security.

5 Conclusion

Secure routing in WSN has been a major challenge due to node mobility and resource constraint nature of such networks. In this paper, we show that identity-based cryptography can play a vital role in defending against many complex cross-layer attacks on WSN routing protocol. As an example, we show how location and energy aware identity-based cryptographic routing can prevent a selective forwarding attack. Additionally, secure cross-layer approach allows intermediate routing nodes to make secure, intelligent routing decisions to prevent route-suppression attacks.

6 Future Work

We have created a secure overlay using the above proposed secure key distribution scheme, but distance measurements using attenuation values are yet to be generated in ASSERT. A working prototype is yet to be constructed and the processing times during secure routing for different topologies are to be calculated.

7 Acknowledgment

The authors would like to thank Ehsan Nourbakhsh for helping us in understanding the ASSERT emulator.

8 References

[1] J. A. Garcia-Maciasx and J. Gomez, "MANET versus WSN," *Sensor Networks and Configuration*, pp. 369-388, 2007.

[2] J. R. Douceur, "The Sybil attack," in *In First International Workshop on Peer-to-Peer Systems (IPTPS '02)*, 2002.

[3] S. Kuo-Feng, W. Wei-Tong, and C. Wen-Chung, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042-3056, Dec. 2009.

[4] H. Kupwade Patil, J. Camp, and S. A. Szygenda, "Identity based authentication using a Cross Layer Design approach in Wireless Sensor Networks," in *World Multiconference on Systemics, Cybernetics and Informatics (WMSCI 2011)*, 2011.

[5] H. Kupwade Patil and S. A. Szygenda, "Identity based key distribution schemes using a Cross Layer Design approach in Wireless Sensor Networks," in *Proc. of Intellectbase International Consortium*, vol. 15, March 2011, pp. 109-118.

[6] Y. Xiao, X. Shen, and D. Du, *Wireless network security*. Springer, 2007.

[7] C. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing for mobile computers," *ACM's Computer Communication Review*, pp. 234-244, 1994.

[8] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90-100.

[9] D. Johnson and D. Maltz, "Dynamic source routing," *Mobile Computing*, pp. 153-181, 1996.

[10] Z. Haas and M. Pearlman, "The performance of query control scheme for the zone routing protocol," *Transactions on Networking*, pp. 427-438, 2001.

[11] Y. Yu, R. Govindan, and D. Estrin, "Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks ," UCLA,

Tech Report, 2001..

[12] D. Aranha, R. Dahab, J. López, and L. Oliveira, "Efficient implementation of elliptic curve cryptography in wireless sensors," *Advances in Mathematics of Communications*, vol. 4, no. 2, pp. 169-187, 2010.

[13] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in *Third International Symposium on Information Processing in Sensor Networks, IPSN*, 2004, pp. 259-268.

[14] A. Shamir, "Identity-based Cryptosystems and Signature Schemes ," *Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science*, vol. 196, pp. 47-53, 1984.

[15] D. Boneh and M. Franklin, "Identity-based encryption from theWeil pairing," *Lecture Notes in Computer Science*, vol. 2139, p. 213–229, 2001.

[16] B. Lee, C. Boyd, E. Dawson, K. Kim, and J. Yang, "Secure Key Issuing in ID-based Cryptography," in *Conferences in Research and Practice in Information Technology*, vol. 32, 2004, pp. 69-74.

[17] F. Hess, "Efficient Identity Based Signature Schemes based on Pairings," *Selected Areas in Cryptography: 9th Annual International Workshop (Lecture Notes in Computer Science)*, vol. 2595, pp. 310-324, 2003.

[18] B. Lynn. (2002) Authenticated Identity-Based Encryption. http://eprint.iacr.org/2002/072/.

[19] R. Sakai, K. Ohgishi , and M. Kasahara, "Cryptosystems based on pairing ,," in *The 2000 Symposium on Cryptography and Information Security*, 2000.

[20] R. Ronald, A. Shamir, and L. Adleman, "A method of obtaining digital signatures and public-key cryptosystems," *Communications*, vol. 21, no. 2, pp. 120-126, 1978.