AN EXPEDITED TRIPLE KEY BROADCAST AUTHENTICATION SCHEME BASED ON TESLA, ECDH, AND ECDSA

[1]M. RAMESH KUMAR, [2]SURESH GNANA DHAS
[1]Research Scholar, Karpagam University, Coimbatore, TamilNadu, India
[2]Professor, Department of Computer Science and Engineering, Vivekananda College of Engineering for Women, Tiruchengode, TamilNadu, India.
E-mail: [1]maestro.ramesh@gmail.com , [2]sureshc.me@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) are prone to various security breaches as they are placed in hostile environments. Several security and broadcast authentication mechanisms were proposed for securing the WSN fully via key exchange mechanisms, handshake protocols, and other routing protocols. But these existing schemes cannot detect a variety of attacks and are not competent in terms of detection accuracy, resiliency, memory consumption, and transmission energy. An expedited triple key broadcast authentication scheme is proposed based on TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol, ECDH (Elliptic Curve Diffie-Hellman) key agreement scheme, and ECDSA (Elliptic Curve Digital Signature Algorithm). The signature verification process is accelerated by releasing few intermediate computation results in the WSN by the sensor nodes. This WSN authentication scheme performs better compared to other security schemes, in terms of accuracy, detection of attacks, resiliency, memory consumption, nodal detection, and average of total transmission energy consumed per node.

Keywords: *Elliptic Curve Diffie-Hellman (ECDH), Signature, ECDSA (Elliptic Curve Digital Signature Algorithm), False positive, Signature, and Timed Efficient Stream Loss-tolerant Authentication (TESLA).*

1. INTRODUCTION

Sensor Networks (WSNs) contain a large number of small sensing nodes. A secure multicast protocol is required to increase the cryptographic strength, authentication and confidentiality. The security in the WSNs is a trivial aspect, which can be enhanced by various measures like key management schemes, signatures, and cryptography methods.

An expedited triple key broadcast authentication scheme is proposed based on TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol, ECDH (Elliptic Curve Diffie-Hellman) key agreement scheme, and ECDSA (Elliptic Curve Digital Signature Algorithm). The signature verification process is accelerated by releasing few intermediate computation results in the WSN by the sensor nodes.

The remaining part of the paper is organized as follows: Section II involves the works related to the broadcast authentication and security schemes in a WSN. Section III involves the detailed analysis of the expedited triple key broadcast authentication scheme in WSN. Section IV involves the security analysis and comparison of the existing and proposed security schemes in a WSN. The paper is concluded in Section V.

2. RELATED WORKS

The various authentication and security mechanisms are discussed in this section. In [1], a bandwidth-effective cooperative authentication (BECAN) is introduced for filtering the false data injection in WSN. This scheme can save energy by the early detection of false data injections. The sink involves only a small fraction of false data injection to be checked. In [2], the HIP DEX scheme is developed by the IETF (Internet Engineering Task Force) to establish a secure WSN. In [3], a novel scheme is developed to maintain the authenticity, secrecy, freshness, and integrity of the broadcast messages in single hop WSNs. This method uses time-varying keys for the broadcast encryption, which results in non-forgeability, allowance for dynamic data, and protection against old-key compromise. The key chain mechanism is also extended to the resistance against key loss, permitting legitimate users to recover. In [4], a security negotiation protocol has been developed for the WSNs based on TLS (Transport Layer Security) handshake. The comparative analyses involve RSA (Rivest-Shamir-Adleman) key transport, Identity Based Encryption and ECDH key agreements.

The WSNs involving the mobile sinks, composite and pairwise key pre-distribution schemes involve a security constraint. In [5], a three-tier framework is used to use any pairwise key pre-distribution scheme as its main component. This scheme requires separate pools for the mobile sink and pairwise key establishment to access the network. In [6], [7] a fast and lightweight pairing-based cryptography method is used in the WSN. A singular elliptic curve is used as the pairing group. The security of the pairing-based cryptosystems depends on the elliptic curve discrete logarithm problem (ECDLP) in the elliptic curve group and discrete logarithm problem in the finite field. The solution to ECDLP is given by Polard's rho method. In [8], the scalability of the key management schemes is focused. A highly scalable key management scheme is proposed based on unital design theory, resulting in high secure connectivity and coverage. The mapping from unitals to key pre-distribution achieves high network scalability. An enhanced unital-based key pre-distribution method is used with a high key sharing probability.

In [9], the problem of pairwise and triple key establishment is focused. A BIBD (Balanced Incomplete Block Design) is used in the combinatorial designs and combinatorial trades to form the pairwise keys between the nodes in a WSN. The pairwise key distribution is fully secure, with low computation, storage, and communication requirements. Strong Steiner Trades are applied in the key management. The concept of triple key distribution between three nodes, allows secure passive surveillance of the forwarding progress in routing tasks. In [10], the group deployment of the keys based on the structure of a resolvable traversal design, results in better connectivity and resilience of the key distribution scheme. In [11], [12] an efficient framework for broadcast authentication is proposed. This framework uses online/offline signatures and identity based cryptography.

In [13], an authentication and key agreement protocol is proposed to reduce the computation and communication costs. The protocol operates through a mobile network which maximizes the lifetime of the sensors in the WSN. In [14], a privacy-preserving and high-energy efficient method is proposed for secure data aggregation. In [15], a secure encrypted-data aggregation technique is proposed for the WSNs. It discards the redundant sensor readings before the encryption. When the sensor readings are encrypted the data aggregation requires decryption, resulting in extra overhead. The duplicate instances of the original sensor readings are aggregated into a single packet. This scheme is resilient to plaintext attacks, ciphertext attacks, and man-in-the-middle attacks.

In [16], the cost of the security in WSN is analyzed. Three features of the WSN security are focused, such as encryption algorithms, message authentication algorithms, and operational mode of blocking ciphers. In [17], critical control systems are used designing various types of ICT (Information and Communication Technology) in Wireless Sensor Mesh Networks. The several communication standards, such as WirelessHART (Highway Addressable Remote Transducer), ISO100.11a, and Zigbee PRO, have been applied to guarantee secure and reliable communications. In [18], the communication standards are enhanced in terms of end-to-end reliability and security.

In [19], a hybrid Intrusion Detection System (IDS) is employed in the cluster head to improve the security of the WSN. It consists of anomaly and interruption detection module to increase the detection rate and decrease the false positive rate. A decision-making module integrates the detection results and reports the type of attacks to the base station. In [20], a practical identity-based encryption technique is proposed known as Receiver-Bounded Online/Offline Identity-based Encryption (RB-OOIBE). The heavy computations are performed during the offline mode, without the knowledge of the plaintext message and receiver's identity. The light computations like, symmetric key encryption and modular operations are performed during the online mode. In [21], a hierarchical key establishment scheme (HIKES) is proposed to increase the organizational efficiency of the key management in the WSN. The base station selects random sensors as local trust authorities and cluster members to issue the private keys. This method deploys a partial escrow method that selects a sensor node (cluster head) to generate the entire keys required to authenticate remaining sensor nodes within the cluster. This technique gives an efficient broadcast authentication with a single transmission source authentication and high flexibility in terms of network connectivity.

In [22], tree-based multicast routing protocols such as, Geographic Multicast Routing (GMR), demand scalable GMR, destination clustering GMR, distributed GMR, sink-initiated GMR, and hierarchical GMR are analyzed. In [23], a three-party password-authenticated key exchange (3PAKE) protocol is proposed based on elliptic curve cryptography. This protocol allows the elements to negotiate a private session key by a trusted server.

3. EXPEDITED TRIPLE KEY AUTHENTICATION

Broadcast authentication in a WSN is an important aspect that permits the legal users to join the network and spread messages into the networks in an authenticated and dynamic manner. Public-key cryptography is used in the implementation of broadcast authentication in WSN and provides high security resilience, scalability and quick message authentication.

3.1 Triple key broadcast authentication

This method provides a secure message authentication mechanism in WSN using TESLA based triple key authentication system reducing the delay and loss. The flow of the triple key broadcast authentication scheme is given in Fig. 1. The nodes are organized and the initial level parameters are set up. The auxiliary key generation is based on a random number and Hilbert number. The auxiliary key generates the signature depending on the auxiliary signature approach. The private/public key generation is based on the ECDH key agreement protocol. The concatenation of these keys results in the hash key, which is broadcasted in the WSN. When the key is validated and estimated to be a valid key, the corresponding node starts to forward the packets to the remaining nodes in the network. When the key is not valid, the packets are discarded and the status is reported to the base station (BS).

The triple key broadcast authentication scheme results in reduced delay and loss. This gradually increases the throughput of the WSN and the delivery ratio of the packets. This model involves a direct pairwise key management scheme between the sensor nodes and the mobile sink. A sensor node determines a stationary access node in its environment, such that it can establish the pairwise keys between the mobile sink and the sensor nodes.

3.2 System Properties

The sensor nodes are limited in its computational, energy, and memory resources and capable of executing various digital signature verification algorithms. The system bootstrapping phase must be secured to avoid compromise attacks. The base station is unbounded in its computational, energy, and memory resources and can implement several cryptographic procedures. The base station is always resistant to compromise attacks.

A densely deployed and static WSN comprising of a base station and many sensor nodes in considered. Multi-hop communication using bidirectional wireless links is preferred owing to the constrained communication capabilities of the devices in the WSN. The users in the WSN can fetch the measurement data of the sensors by broadcasting commands and queries into the network. Also, the users require registering and obtaining security certificates for the broadcast services.

3.3 User broadcast in WSN

Elliptic Curve Digital Signature Algorithm (ECDSA) is used to quicken the signature verification process based on coordination between the sensor nodes. A user requests its neighboring sensor nodes for broadcast services after registering and obtaining the security certificates. The sensor nodes perform a mutual authentication process that authorizes the WSN access only to an authenticated user. The user needs to sign the command/query before transmitting it to the sensor nodes. The process of broadcast from the user to the sensor nodes is illustrated in Fig. 2.

The user signs a command or query and forwards it to the various sensor nodes. In our case, nodes A, B, C, and D receive the command/query and verify its signature. Further local broadcast of the user's command/query happens only when the signature verification is successful. When the neighboring node of C receives the broadcast packet for the first time i.e. E, it will also undergo the same signature verification to determine whether the packet can be forwarded to the next nodes. When a signature verification process fails, the sensor node drops the packet and informs the base station.

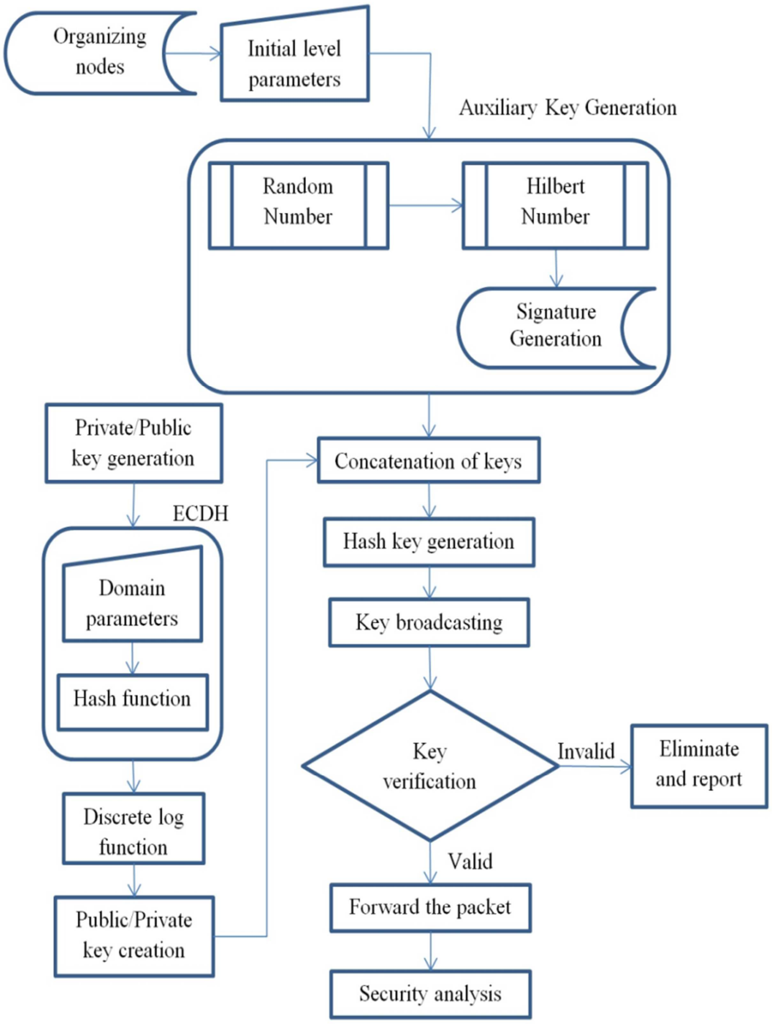

Fig. 1. Flow Of The Triple Key Broadcast Authentication Scheme.

3.4 Advancing the signature verification

The verification of an ECDSA signature involves the computation of two scalar multiplication processes M_1 and M_2. The signature verification can be accelerated significantly when the sensor nodes release few intermediate results. This will also decrease the overall energy consumption of the WSN.

The nodes E and F which are the neighbors of nodes C and D respectively can verify the digital signature by elliptic curve point addition of M_1 and M_2. M_1 is computed by nodes C and D, whereas M_2 is computed by nodes E and F. When a sensor node releases its intermediate multiplication results, all its neighboring nodes can accelerate the digital signature verification by just computing one scalar multiplication and one elliptic curve point addition. When the sensor nodes utilize two intermediate computation values for signature verification, they may receive any bogus broadcast message from an attacker. To prevent this attack, the sensor nodes are permitted to use at most only one intermediate value (M_1 or M_2) from the neighboring nodes.

3.5 Algorithm for faster ECDSA signature verification

The redundancy of broadcast packets attributes to the faster signature verification. The algorithm for faster ECDSA signature verification is given in ALGORITHM I.

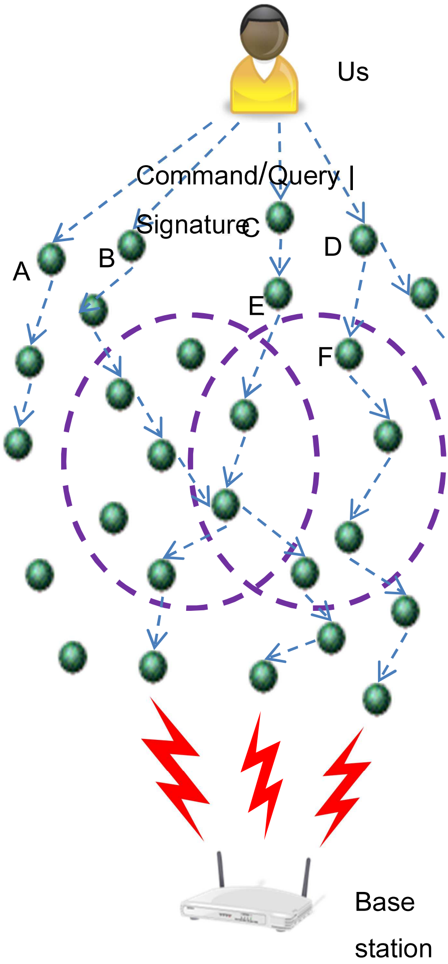

Fig. 2. Process of broadcast from the user to the sensor nodes.

Initially each sensor node waits for *t* seconds and caches *d* data packets received from its neighboring nodes. The sensor node that determines whether the cached *d* data packets have identical query, signature, and M_2.

- When the received data packets have different query, signature, or M_2, the sensor node will report the possible attack to the base station.
- When the cached *d* data packets have identical query, signature, and M_2, the sensor node will further see whether it was obtained the useful data packets.

ALGORITHM I – Faster ECDSA Signature Verification

```
Input: Data packages for sensor nodes in WSN, $M_1$ and $M_2$ → Scalar multiplications, $t$ → delay, $d$ → threshold packets, and $P_r$ → Release probability.
Output: Signed broadcast packages
begin
    for each package
        if (type = random)
            Discard package
            end
        else
            if new package
                Wait for $t$ seconds and cache $d$ packages
                if $d$ packages have different query, signature, and $M_2$
                    Discard $d$ packages and report to BS
                    end
                else
                    if $d$ packages don't contain query, signature, and $M_2$ in the data packet
                        Compute $M_1$ and $M_2$
                        Compute $M_1 + M_2$
                        Verify the signature
                    else
                        Compute $M_1$
                        Compute $M_1 + M_2$
                        Verify the signature
                    end if-else
                end if-else
            end if-else
            if verification is successful
                Release $M_2$ with probability $P_r$
                Forward the signed broadcast package
            else
                Discard the package and report to BS
                end
            end if-else
        end if-else
    end for
end
```

The sensor node will compute M_1 and then complete the signature verification with one scalar multiplication and one elliptic curve point addition.

3.6 Selection of delay t and threshold d

The number of neighbors for sensor node *E* is denoted as *α* and half of them will be used to broadcast data packets to *E* in rounds. Node *E*'s *α*/2 neighbors *β* nodes can be compromised by attackers and each of them can transmit at most x bogus data packets to E. The threshold value d should satisfy the following condition to avoid collusive attacks from adversaries.

$$\alpha/2 \geq d \geq \beta\,(x+1)$$

This ensures that node E does not admit any bogus messages for collusive attackers as the entire cached data are different. The delay t is chosen according to the following condition after the determination of threshold d, such that the data packets can be received by the sensor node E.

$t \geq t_d.\ d,$ where t_d is the radio backoff of the transceiver.

3.7 Computation of average release probability $\mathbf{P_M}$

A sensor node will release its intermediate result based on the individual release probability P_r. A trade-off exists between the signature verification speed and energy consumption of the WSN, so an optimum P_r is chosen. For a group of N sensor nodes processing on signature verification at each round the average release probability that M nodes will release their intermediate results is given by P_M.

$$P_M = \binom{N}{M}.\,P_r{}^{\mathrm{T}}.\,(1-P_r)^{(N-M)}$$

3.9 Change in energy consumption due to faster signature verification

The energy consumption while M sensor nodes locally broadcast their intermediate results is equal to $M * E_t$, where E_t is the energy consumption of transmitting a packet. The energy consumption of approximately $\alpha M/2$ nodes receiving the intermediate computations is equal to $\alpha M/2 * E_r$, where E_r is the energy consumption of receiving a packet. The energy consumption of approximately $\alpha M/2$ nodes advancing their signature verification using the received intermediate results is equal to $\alpha M/2 * E_m$, where E_m is the energy consumption of computing one elliptic curve multiplication on the nodes. The change in energy consumption due to the faster signature verification is given by an energy term e.

$$e = \sum_{M=1}^{N} P_M \left(ME_t + \frac{\alpha M}{2} E_r - \frac{\alpha M}{2} E_m \right)$$

The release probability P_r is chosen according to the value of e which will minimize the energy consumption when e is positive or maximize the energy saving when e is negative.

4. SECURITY ANALYSIS

The expedited triple key broadcast authentication scheme is compared with various existing broadcast authentication and security schemes in WSN. The network architecture composes of 300 nodes in a simulated area of 10003 * 1000 m. The nodal velocity is varied from 5 to 30 m/s. They are analyzed in terms of communication overhead, energy consumption and time taken for various cryptographic processes, such as key setup, encryption, decryption, key extraction, signature establishment, and signature verification. The detection rate of attacks in the WSN is analyzed in terms of the detection accuracy and its false positive rate (FPR). The various techniques are also compared in terms of capability of detecting various attacks, memory consumption, resiliency, and the probability of hash value being compromised versus the number of compromised nodes.

4.1 Communication overhead

The communication overhead for a high energy-efficient and privacy preserving (HEEPP) secure data aggregation scheme [14] and the expedited triple key broadcast authentication scheme is compared in Fig. 3.

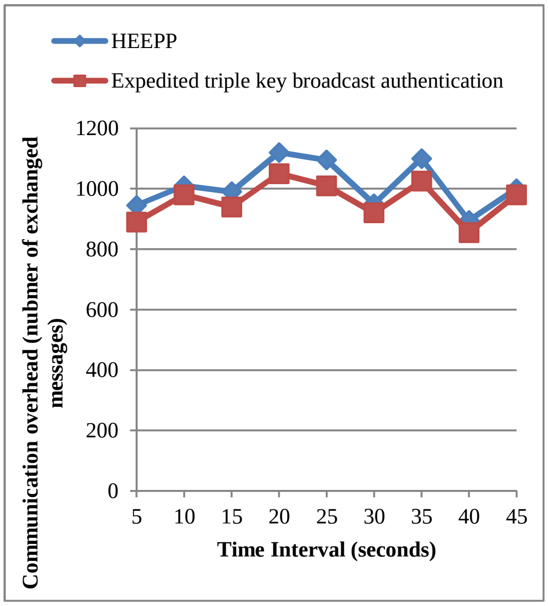

Fig. 3. Comparison Of Communication Overhead.

4.2 Detection of various attacks in a WSN

The capability of detecting various attacks in a WSN by HIKES protocol [21] and the expedited triple key broadcast authentication scheme is compared in TABLE I. The various attack detection rates for a hybrid intrusion detection system (IDS) in a cluster-based WSN [19] and the expedited triple key based authentication scheme is compared in TABLE II. The performance evaluation of the hybrid IDS [19] and the expedited triple key broadcast authentication scheme is given in TABLE III.

Table I Capability Of Detecting Various Attacks In A Wsn

Attacks	HIKES	Expedited triple key broadcast authentication
Routing information	✔	✔
Selective forwarding	✖	✔
Sinkhole attacks	✔	✔
Sybil attacks	✔	✔
Wormholes	✔	✔
HELLO flood attacks	✔	✔
Acknowledgement spoofing	✖	✔

Table II Detection Rate For Various Attacks In A Wsn

Attacks	Hybrid IDS	**Expedited triple key broadcast authentication**
Normal	99.43%	**99.512%**
Probe	99.20%	**99.345%**
DoS (Denial of Service)	99.99%	**99.992%**
U2R (User-to-Root)	58.82%	**63.548%**
R2L (Remote-to-Local)	97.60%	**98.265%**

Table III Performance Evaluation

Parameter	Hybrid IDS	**Expedited triple key broadcast authentication**
Detection rate	99.81%	**99.856%**
False positive	0.57%	**0.235%**
Accuracy	99.75%	**99.814%**

4.3 Total storage

The total storage for HIKES protocol [21] is 726 bytes, sensor node authentication in 3G-WSN [13] is 33 bytes, while for the expedited triple key broadcast authentication scheme it is 25 bytes.

4.4 Energy consumption and time taken for various cryptographic processes

The energy consumed by NU-KP (Native Unital based Key Predistribution) [8] and the expedited triple key broadcast authentication scheme, for the specified network size is given in Fig. 4. The difference in energy consumption and time consumption of various cryptographic processes using AES (Advanced Encryption Standard) algorithm [16] and SHA1 (Secure Hash Algorithm

1) algorithm used in the expedited triple key broadcast authentication scheme is compared in TABLE IV. The difference in energy consumption and time consumption of various cryptographic processes using AES (Advanced Encryption Standard) algorithm [16] and SHA1 (Secure Hash Algorithm 1) algorithm used in the expedited triple key broadcast authentication scheme is compared in TABLE V.

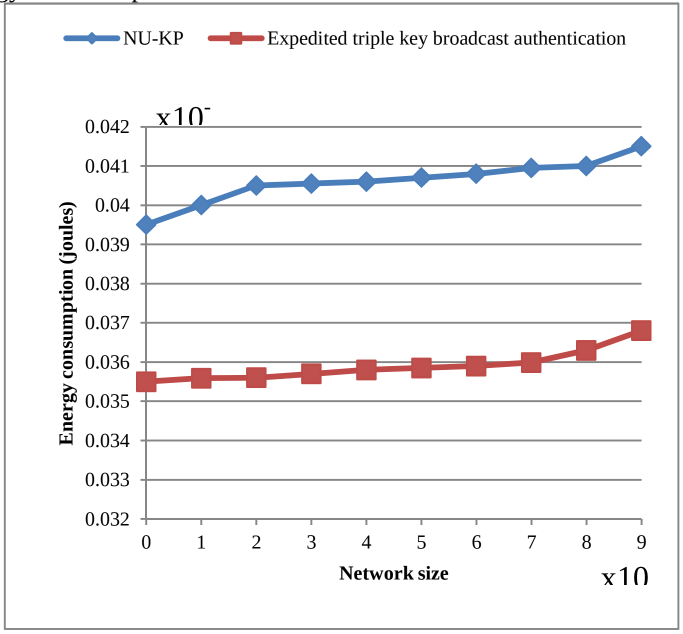

Fig. 4. Energy Consumption For NU-KP And Expedited Triple Key Based Broadcast Authentication Scheme.

Table IV: Time Taken For Various Cryptographic Processes By Tinypairing And Triple Key Broadcast Authentication

Cryptographic process	TinyPairing	Key-chain based encryption in single hop WSN	**Expedited triple key broadcast authentication**
Initialization	12.33 s	53.2 s	**2.56 ms**
Signature	3.0 s	35.7 s	**1.25 ms**
Verification	11.03 s	59.8 s	**2.42 ms**
Key extraction	2.83 s	n/a	**1.16 ms**
Encryption	10.59 s	n/a	**2.98 ms**
Decryption	5.34 s	n/a	**35.41 ms**
Signature size	312 bits	-	**256 bits**
Sending message to BS	n/a	3.7 s	**0.59 ms**
Diffie-Hellman key exchange	-	5.5 s	**1.32 ms**

n/a: not available.

Table V Difference Between Aes And Sha1 Algorithms

Algorithm	Key Setup		Encryption		Decryption	
	(ms)	(µJ)	(ms)	(µJ)	(ms)	(µJ)
AES	3.58	26.74	3.77	28.16	43.20	322.70
SHA1	**2.56**	**24.35**	**2.98**	**27.54**	**35.41**	**221.48**

4.5 Probability of hash value being compromised vs. number of compromised nodes

The probability of hash value being compromised is observed for different number of compromised nodes. The comparison is made between the expedited triple key broadcast authentication scheme and a three-tier security scheme in WSN with mobile sinks [5], and is shown in Fig. 5.

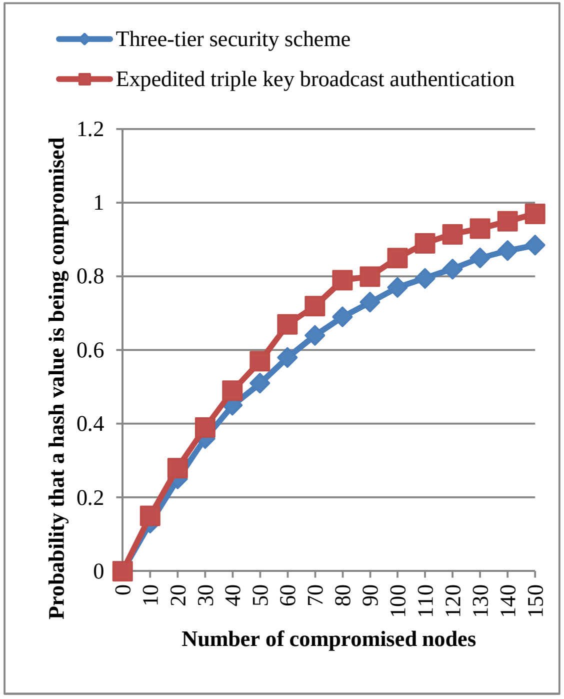

Fig. 5. Probability Of Hash Value Being Compromised Vs. The Number Of Compromised Nodes.

4.6 Resiliency of network

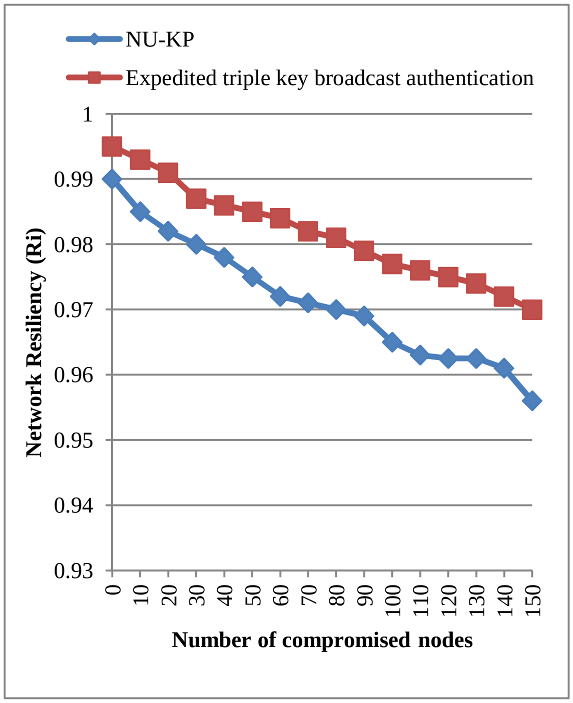

Fig. 6. Network Resiliency For NU-KP And Expedited Triple Key Broadcast Authentication Scheme.

Network resiliency (R_i) is defined as the ratio of uncompromised external secure connections when *i* sensor nodes are captured. The network resiliency (R_i) is observed for NU-KP [8] and the expedited triple key broadcast authentication scheme is compared in Fig. 6.

5. CONCLUSION

Wireless Sensor Networks (WSNs) are prone to various attacks because of their hostile environment. The security of a WSN is critical especially in military communications. The expedited triple key broadcast WSN authentication is based on TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol, ECDH (Elliptic Curve Diffie-Hellman) key agreement scheme, and ECDSA (Elliptic Curve Digital Signature Algorithm). The signature verification process is accelerated by releasing few intermediate computation results in the WSN by the sensor nodes. It performs better compared to other security schemes, in terms of accuracy, detection of attacks, resiliency, memory consumption, nodal detection, and average of total transmission energy consumed per node.

REFERENCES:

[1] L. Rongxing, *et al.*, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," *Parallel and Distributed Systems, IEEE Transactions on*, 2012, vol. 23, no. 1, pp. 32-43.

[2] P. Nie, *et al.*, "Performance analysis of HIP diet exchange for WSN security establishment," presented at the *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks*, Miami, Florida, USA, 2011.

[3] V. Sivaraman, *et al.*, "Broadcast secrecy via key-chain-based encryption in single-hop wireless sensor networks," *EURASIP J. Wirel. Commun. Netw.*, 2011, vol. 2011, pp. 1-12.

[4] G. Bianchi, *et al.*, "Flexible key exchange negotiation for wireless sensor networks," presented at the *Proceedings of the fifth ACM international workshop on Wireless network testbeds, experimental evaluation and characterization*, Chicago, Illinois, USA, 2010.

[5] A. Rasheed and R. N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks," *Parallel and Distributed Systems, IEEE Transactions on*, 2012, vol. 23, no. 5, pp. 958-965.

[6] X. Xiaokang, *et al.*, "TinyPairing: A Fast and Lightweight Pairing-Based Cryptographic Library for Wireless Sensor Networks," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, 2010, pp. 1-6.

[7] L. B. Oliveira, *et al.*, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Computer Communications*, 2011, vol. 34, no. 3, pp. 485-493.

[8] W. Bechkit, *et al.*, "A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks," *Wireless Communications, IEEE Transactions on*, 2013, vol. 12, no. 2, pp. 948-959.

[9] S. Ruj, *et al.*, "Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs," in *INFOCOM, 2011 Proceedings IEEE*, 2011, pp. 326-330.

[10] K. M. Martin, *et al.*, "Key predistribution for homogeneous wireless sensor networks with group deployment of nodes," *ACM Trans. Sen. Netw.*, 2010, vol. 7, no. 2, pp. 1-27.

[11] R. Yasmin, *et al.*, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 882-889.

[12] J. Liu, *et al.*, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, 2010, vol. 9, no. 4, pp. 287-296.

[13] K. Han, *et al.*, "Efficient sensor node authentication via 3GPP mobile communication networks," presented at the *Proceedings of the 17th ACM conference on Computer and communications security*, Chicago, Illinois, USA, 2010.

[14] C.-X. Liu, *et al.*, "High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks," *International Journal of Communication Systems*, 2013, vol. 26, no. 3, pp. 380-394.

[15] S.-I. Huang, *et al.*, "Secure encrypted-data aggregation for wireless sensor networks," *Wireless Networks*, 2010, vol. 16, no. 4, pp. 915-927.

[16] J. Lee, *et al.*, "The price of security in wireless sensor networks," *Computer Networks*, 2010, vol. 54, no. 17, pp. 2967-2978.

[17] C. Alcaraz and J. Lopez, "A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 2010, vol. 40, no. 4, pp. 419-428.

[18] L. Buttyan and L. Csik, "Security analysis of reliable transport layer protocols for wireless sensor networks," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on*, 2010, pp. 419-424.

[19] K. Q. Yan, *et al.*, "Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, 2010, pp. 114-118.

[20] C.-K. Chu, *et al.*, "Practical ID-based encryption for wireless sensor network," presented at the *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, Beijing, China, 2010.

[21] J. Ibriq and I. Mahgoub, "HIKES: Hierarchical key establishment scheme for wireless sensor networks," *International Journal of Communication Systems*, 2012, pp. 1-32.

[22] M. Bala Krishna and M. N. Doja, "Analysis of tree-based multicast routing in wireless sensor networks with varying network metrics," *International Journal of Communication Systems*, 2012, pp. 1-14.

[23] M. A. Simplicio and R. R. M. Sakuragui, "Cryptanalysis of an efficient three-party password-based key exchange scheme," *International Journal of Communication Systems*, 2012, vol. 25, no. 11, pp. 1443-1449.