An Analysis of Broadcast Authentication and Security Schemes in Wireless Sensor Networks

M.Ramesh Kumar [#1], Dr.C.Suresh Gnana Dhas[*2]

[#]Research Scholar, Karpagam University, Coimbatore, TamilNadu, India.
E-mail: maestro.ramesh@gmail.com.
[*]Professor, Department of Computer Science and Engineering, Vivekananda College of Engineering for Women, Tiruchengode, Tamil Nadu, India.
E-mail: sureshc.me@gmail.com

***Abstract*— Wireless Sensor Networks (WSNs) are susceptible to various attacks as they are placed in hostile environments. Several security and authentication mechanisms are proposed for in terms of key exchange mechanisms, handshake protocols, and other routing protocols. The proposed triple key based broadcast authentication protocol is compared with the several other existing security schemes in WSN. The proposed triple key based broadcast authentication scheme works upon TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol and ECDH (Elliptic Curve Diffie-Hellman) key agreement scheme. The proposed WSN authentication 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.**

Keyword- Base Station1, Elliptic Curve Diffie-Hellman2, Signature3, Timed Efficient Stream Loss-Tolerant4, Wireless Sensor Networks5.

I. INTRODUCTION

Wireless 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 like Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol. Some of the techniques are analysed and compared with the proposed triple key management scheme using TESLA (Timed Efficient Stream Loss-tolerant Authentication) broadcast authentication protocol.

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 existing and proposed broadcast authentication and security schemes in a 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.

II. RELATED WORK

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 focussed. 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 focussed. 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 analysed. Three features of the WSN security are focussed, 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 analysed. 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.

III. Broadcast Authentication and Security Schemes in WSN

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.

A. Proposed Triple Key Broadcast Authentication Scheme

This method provides a secured message authentication mechanism in WSN using TESLA based triple key authentication system reducing the delay and loss. The flow of the proposed model is given in Figure 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 proposed triple key broadcast authentication scheme gives reduced delay and loss. This gradually increases the throughput of the WSN and the delivery ratio of the packets. The proposed 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.

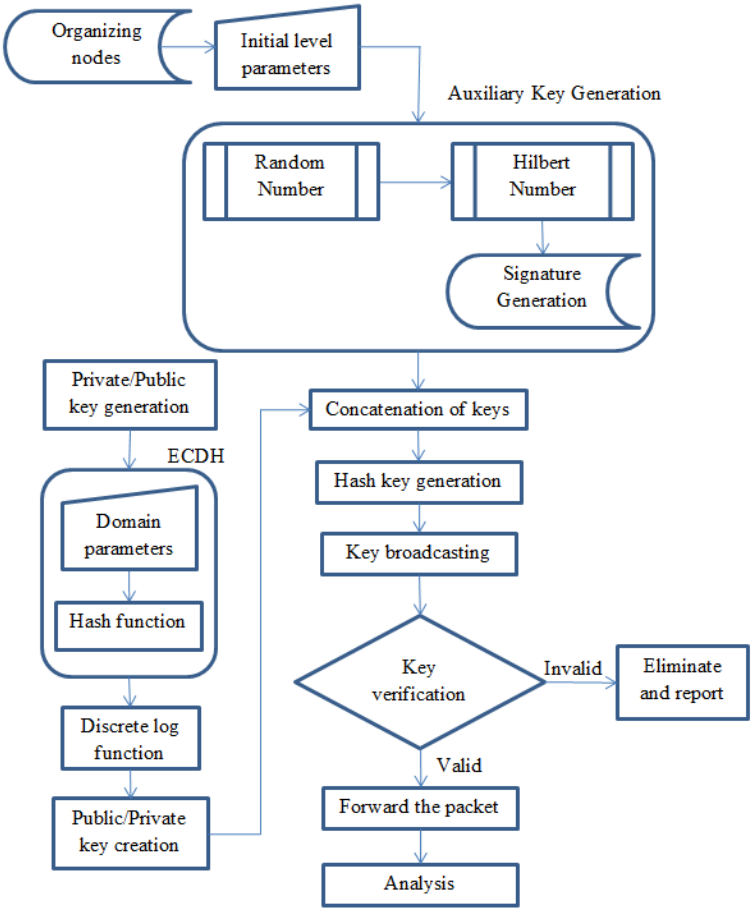

Figure 1. Working of the proposed three-key authentication scheme.

B. Bandwidth-Efficient Cooperative Authentication (BECAN) Model for WSN

An efficient BECAN model is used to counter the false data attacks in a WSN [1]. The BECAN authentication process consists of two steps: initialization and deployment of sensor nodes, and reporting of sensed results. The *sink* (data collection device) chooses an elliptic curve ($\mathbf{E}(A_p)$, S, m) defined over the region A_p, where p is a large prime and $S \in \mathbf{E}(A_p)$ is a base point of prime order m, under the specified security parameter κ. The *sink* chooses a secure cryptographic hash function $h()$ and then sets the public parameters $\{\mathbf{E}(A_p), S, m, h()\}$. The *sink* initializes the set of sensor nodes and deploys them uniformly at specific regions of interest.

The sensor nodes report the sensed data i to the sink via an established routing path. The sensed data is sent along with a timestamp T by the source node. The sensed data i combined with the timestamp T and routing path R, and this acts as the input for each individual sensor node in the routing path. Each sensor node along R generates a row authentication vector. The source node aggregates all the row vectors generated by the sensor nodes and forms the MAC (Message Authentication Code).

When a sensor node along the routing path R receives (i, T, MAC) from its predecessor node, the integrity of the timestamp and the sensed data is checked. When the timestamp is out of date, the message (i, T, MAC) is discarded; else the message is forwarded to the next node. When the *sink* receives the report (i, T, MAC) the integrity of the timestamp and the sensed data is checked. When the timestamp is out of date, the message (i, T, MAC) is immediately discarded; else the set of private keys is verified by the *sink*.

Multi-reports solution is used to enhance the reliability of the reception of the sensed data, i.e., the multi-source nodes near the sensing event choose various neighbours, and send the generated multi-reports to the *sink*.

When a single report reaches the *sink*, the sensing event will be successfully reported.

C. HIP DEX for Enhanced Security in WSN

HIP (Host Identity Protocol) Diet Exchange (DEX) scheme is a generic solution for the securing the WSN [2]. This scheme consists of four messages to construct a secure direct connection between two neighbour nodes, the sender and the receiver respectively. The flow of the four messages is shown in Figure 2.

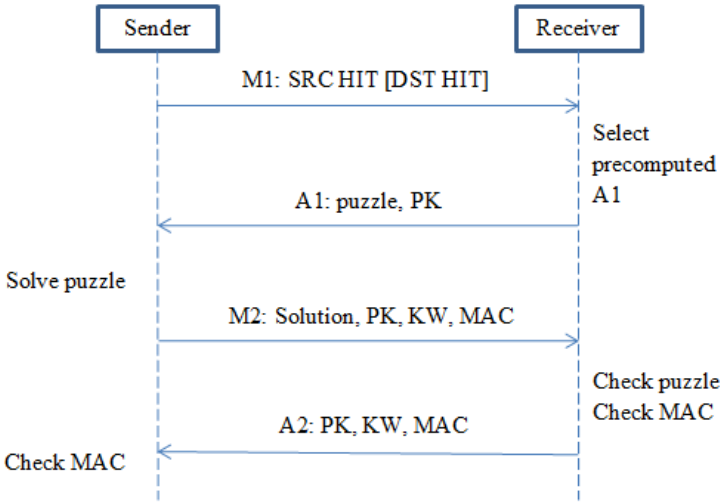

Figure 2. Timing diagram of HIP DEX scheme.

The first message M1 contains the source host identity tag (HIT) and an optional destination HIT (DST HIT). The second message A1 contains a puzzle, i.e., a cryptographic challenge to the sender and also defines the encryption algorithms supported by the receiver. The third message M2 contains the solution to the puzzle and a key wrap variable (KW). M2 is MACed to guarantee the message integrity against tampering conditions. The fourth message A2 containing another key wrap variable KW, is also MACed to finalize the handshake. The messages M2 and A2 comprise an authenticated secret key wrapped by ECDH, for the generation of session keys to encrypt the subsequent data packets.

The HIP DEX scheme specifies a state machine to control the state transitions until a security association (SA) is guaranteed. This scheme involves data encryption, identity authentication, and message integrity. The authentication of the sending and receiving nodes is enhanced by the session key generated from the ECDH handshake. The lack of digital signature in this scheme implies the receiver's identity cannot be validated by the sender. Thus, the A1 message is not protected and can be hacked. Cipher-based MAC (CMAC) guarantees the message integrity.

D. Key-Chain Based Encryption in Single Hop WSN

The key chain encryption scheme of broadcasting packets in a single hop WSN is shown in Figure 3 [3]. The base station (BS) chooses an arbitrary key k_X for the generation of the key chain k_X, k_{X-1},…, k_1, k_0. The key k_{n-1} is a hash function $H(k_n)$ for n = 1,…, X. The hash function can be SHA1 (Secure hash algorithm) or MD5 (Message Digest). The root key k_0 needs to be securely transmitted to each target node. When the target nodes receive the key node, the BS forms the first broadcast packet by integrating the broadcast data and the succeeding key k_1, and encrypts the message with a symmetric encryption method using the root key. The encrypted packet is broadcast to all the nodes in the WSN. The offset code-book (OCB) block cipher encryption method guarantees that the encrypted key and encrypted data are inseparable in cipher text. The receiver node decrypts the message using the root key. The condition $H(k_1) = k_0$ is checked to verify the integrity and authenticity of the packet's source. The root key k_0 is now discarded and is replaced by the new key k_1. These steps are repeated for the entire key chain k_i, where i = 1, 2, …. The successive packets must be transmitted at such a rate that gives the nodes enough time to extract the data payload. The generation of the new key chain is initiated once all the X broadcast packets have been sent.

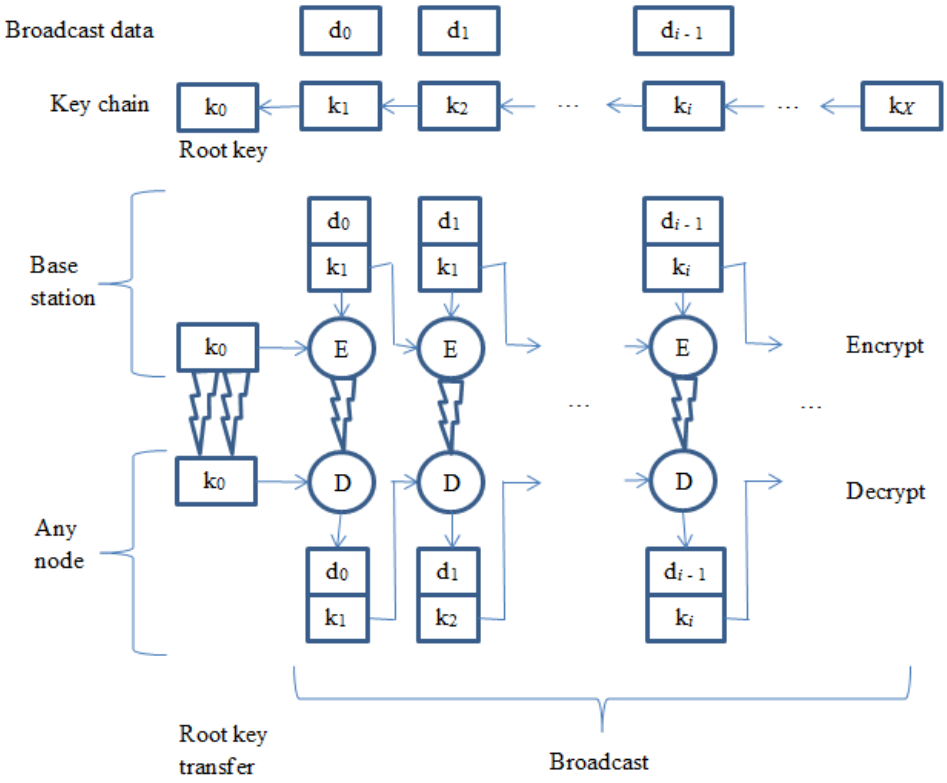

Figure 3. Key chain encryption of broadcast packets in single hop WSN.

The public-key cryptography for the secure communication of the root key is implemented in a bootstrap phase using elliptic-curve public-key cryptography. The BS and the sensor nodes hold a pair of public/private key. The public keys are required only during the bootstrap phase. A secure channel can be established using an authenticated Diffie-Hellman (DH) exchange. The BS initiates the DH exchange by sending a digitally signed message involving its transient key component and the target sensor node replies with its own signed transient key component. The transient nature of the shared key protects the DH exchange against capture-and-replay attacks. The digital signature preserves the authentication and protects against man-in-the-middle attacks.

A disadvantage in the key-chain approach is that a receiver which losses even one broadcast packet is removed from all the future broadcast messages. This problem arises because the key inside the missing packet is required to decrypt the subsequent packet containing the key to the next packet. The loss of the key contained in the packet is an issue in unreliable broadcast scenarios. A scheme for the recovery of the lost keys should have the following properties: The recovery scheme should be operated at low computational cost, limiting the ability of the intruder, and the receivers should be decision independent.

A recovery field is appended to the data field in the packets to be transmitted. The recovery field contains the next key k_{n+1}, an integer $x \geq 1$, and the hash digest $H(k_{n+1} \mid x)$. The node which has missed x former broadcast packets, is allowed to use its old key to shift forward in the chain and recover the next key to be used. The integer x is chosen according to a geometric distribution given by $(1 - y)^{x-1}y$ for a parameter $y \in (0, 1)$. The advantage of this recovery scheme is that it does not involve radio transmissions but only local computations at the receivers.

E. Key Exchange Negotiation in WSN

A key exchange protocol should be security-oriented rather than session-oriented, and minimize the transmission overhead and energy consumption [4]. Figure 4 shows the negotiation procedure in the key exchange process. The sender node initiates the security association setup with a SENDERHELLO message and the RECEIVERHELLO message specifies the employed cipher suite. The FINISHED message consists of HMAC (Hash-based MAC) computed over the entire set of messages exchanged during the handshake, with the master key calculated at the end of the key-exchange. The HMAC is derived from the pre-master secret agreed upon by ECDH. The HMAC size is dependent on the digest size of the hash function. The messages transferred after the RECEIVERHELLO message depend on the negotiated asymmetric algorithm, and may include a KEYEXCHANGE message.

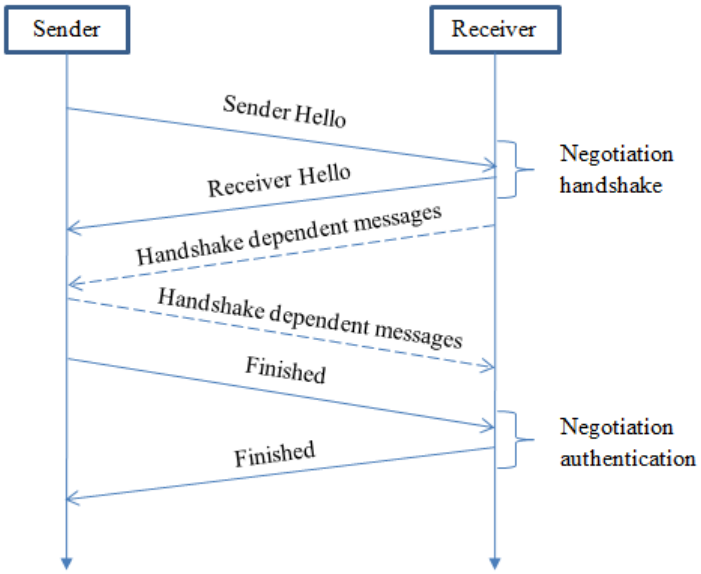

Figure 4. Cipher suite negotiation.

IV. Security Analysis

The proposed triple key broadcast authentication scheme is compared with various existing broadcast authentication and security schemes in WSN. The network architecture considered in the proposed model 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 analysed 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 analysed 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.

A. Communication Overhead

The communication overhead for a high energy-efficient and privacy preserving (HEEPP) secure data aggregation scheme [14] and the proposed triple key broadcast authentication scheme is compared in Figure 5.

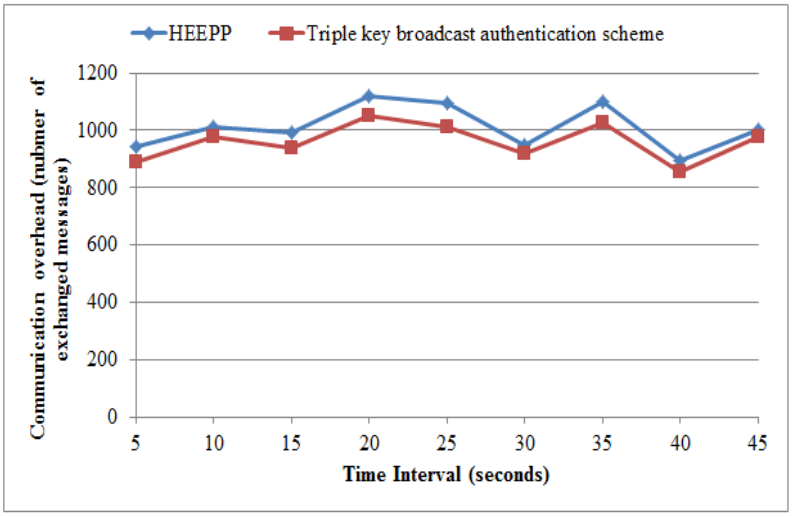

Figure 5. Comparison of communication overhead.

B. Detection of Various Attacks in a WSN

The capability of detecting various attacks in a WSN by HIKES protocol [21] and the proposed 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 proposed triple key based authentication scheme is compared in TABLE II. The performance evaluation of the hybrid IDS [19] and the proposed triple key broadcast authentication scheme is given in TABLE III.

Table II. Detection rate for various attacks in a WSN.

Attacks	Hybrid IDS [19]	Proposed 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 [19]	Proposed triple key broadcast authentication
Detection rate	99.81%	99.856%
False positive	0.57%	0.235%
Accuracy	99.75%	99.814%

TABLE I. Capability of Detecting Various Attacks in a WSN.

Attacks	HIKES [21]	Proposed triple key broadcast authentication
Routing information	Yes	Yes
Selective forwarding	No	Yes
Sinkhole attacks	Yes	Yes
Sybil attacks	Yes	Yes
Wormholes	Yes	Yes
HELLO flood attacks	Yes	Yes
Acknowledgement spoofing	No	Yes

C. 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 proposed triple key broadcast authentication scheme it is 25 bytes.

D. Energy Consumption and Time Taken for Various Cryptographic Processes

The energy consumed by NU-KP (Native Unital based Key Predistribution) [8] and the proposed triple key broadcast authentication scheme, for the specified network size is given in Figure 6. 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 proposed model 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 proposed model is compared in TABLE V.

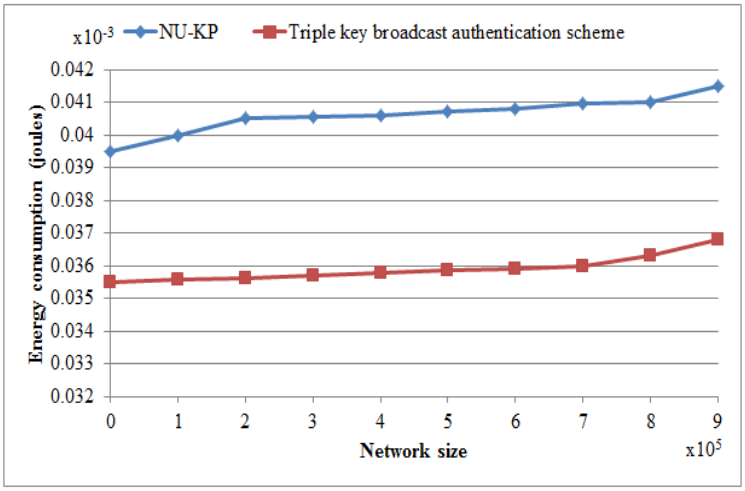

Figure 6. Energy consumption for NU-KP [8] and proposed triple key based broadcast authentication scheme.

Table V. Difference Between Aes and Sha1 Algorithms.

Algorithm	Key Setup		Encryption		Decryption	
	(ms)	(μJ)	(ms)	(μJ)	(ms)	(μJ)
AES [16]	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

Table IV.
Time taken for various cryptographic processes by TinyPairing [6] and the proposed triple key broadcast authentication.

Cryptographic process	TinyPairing [6]	Key-chain based encryption in single hop WSN [3]	Proposed triple key broadcast authentication
Initialisation	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.

E. 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 proposed triple key broadcast authentication scheme and a three-tier security scheme in WSN with mobile sinks [5], and is shown in Figure 7.

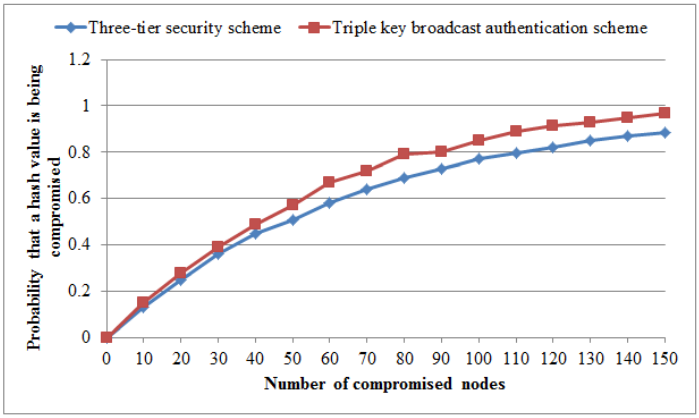

Figure 7. Probability of hash value being compromised vs. the number of compromised nodes.

F. Resiliency of Network

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 proposed triple key broadcast authentication scheme is compared in Figure 8.

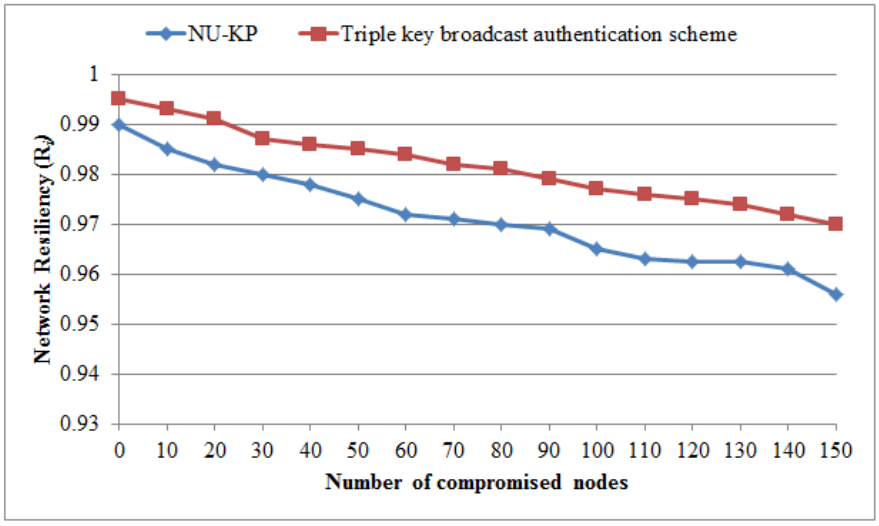

Figure 8. Network resiliency for NU-KP [8] and proposed triple key broadcast authentication scheme.

V. 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. Several authentication and security schemes are used for enhancing the WSN security. The proposed triple key based broadcast authentication protocol is developed upon Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme and TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol. The proposed WSN authentication 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] Rongxing L, Xiaodong L, Haojin Z, Xiaohui L, Xuemin S. BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks. *Parallel and Distributed Systems, IEEE Transactions on*. 2012; 23(1):32-43, DOI: 10.1109/tpds.2011.95.

[2] Nie P, V J, #228, -Herttua, Aura T, Gurtov A. *Performance analysis of HIP diet exchange for WSN security establishment.* Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks; Miami, Florida, USA: ACM; 2011. 51-56, DOI: 10.1145/2069105.2069114.

[3] Sivaraman V, Ostry D, Shaheen J, Hianto AJ, Jha S. Broadcast secrecy via key-chain-based encryption in single-hop wireless sensor networks. *EURASIP J Wirel Commun Netw*. 2011; 2011:1-12, DOI: 10.1155/2011/695171.

[4] Bianchi G, Capossele AT, Mei A, Petrioli C. *Flexible key exchange negotiation for wireless sensor networks*. Proceedings of the fifth ACM international workshop on Wireless network testbeds, experimental evaluation and characterization; Chicago, Illinois, USA: ACM; 2010. 55-62, DOI: 10.1145/1860079.1860090.

[5] Rasheed A, Mahapatra RN. The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks. *Parallel and Distributed Systems, IEEE Transactions on*. 2012; 23(5):958-965, DOI: 10.1109/tpds.2010.185.

[6] Xiaokang X, Wong DS, Xiaotie D. *TinyPairing: A Fast and Lightweight Pairing-Based Cryptographic Library for Wireless Sensor Networks*. Wireless Communications and Networking Conference (WCNC), 2010 IEEE; 2010, 18-21 April 2010, DOI: 10.1109/wcnc.2010.5506580.

[7] Oliveira LB, Aranha DF, Gouvêa CPL, Scott M, Câmara DF, López J, et al. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. *Computer Communications*. 2011; 34(3):485-493, DOI: 10.1016/j.comcom.2010.05.013.

[8] Bechkit W, Challal Y, Bouabdallah A, Tarokh V. A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks. *Wireless Communications, IEEE Transactions on*. 2013; 12(2):948-959, DOI: 10.1109/twc.2012.010413.120732.

[9] Ruj S, Nayak A, Stojmenovic I. *Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs*. INFOCOM, 2011 Proceedings IEEE; 2011, 10-15 April 2011, DOI: 10.1109/infcom.2011.5935175.

[10] Martin KM, Paterson MB, Stinson DR. Key predistribution for homogeneous wireless sensor networks with group deployment of nodes. *ACM Trans Sen Netw*. 2010; 7(2):1-27, DOI: 10.1145/1824766.1824767.

[11] Yasmin R, Ritter E, Guilin W. *An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures*. Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on; 2010, June 29 2010-July 1 2010, DOI: 10.1109/cit.2010.165.

[12] Liu J, Baek J, Zhou J, Yang Y, Wong J. Efficient online/offline identity-based signature for wireless sensor network. *Int J Inf Secur*. 2010, 2010/08/01; 9(4):287-296, DOI: 10.1007/s10207-010-0109-y.

[13] Han K, Kim J, Kim K, Shon T. *Efficient sensor node authentication via 3GPP mobile communication networks*. Proceedings of the 17th ACM conference on Computer and communications security; Chicago, Illinois, USA. 1866398: ACM; 2010. 687-689, DOI: 10.1145/1866307.1866398.

[14] Liu C-X, Liu Y, Zhang Z-J, Cheng Z-Y. High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks. *International Journal of Communication Systems*. 2013; 26(3):380-394, DOI: 10.1002/dac.2412.

[15] Huang S-I, Shieh S, Tygar JD. Secure encrypted-data aggregation for wireless sensor networks. *Wireless Netw*. 2010, 2010/05/01; 16(4):915-927, DOI: 10.1007/s11276-009-0177-y.

[16] Lee J, Kapitanova K, Son SH. The price of security in wireless sensor networks. *Computer Networks*. 2010; 54(17):2967-2978, DOI: 10.1016/j.comnet.2010.05.011.

[17] Alcaraz C, Lopez J. 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; 40(4):419-428, DOI: 10.1109/tsmcc.2010.2045373.

[18] Buttyan L, Csik L. *Security analysis of reliable transport layer protocols for wireless sensor networks*. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on; 2010, March 29 2010-April 2 2010, DOI: 10.1109/percomw.2010.5470633.

[19] Yan KQ, Wang SC, Wang SS, Liu CW. *Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network*. Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on; 2010, 9-11 July 2010, DOI: 10.1109/iccsit.2010.5563886.

[20] Chu C-K, Liu JK, Zhou J, Bao F, Deng RH. *Practical ID-based encryption for wireless sensor network*. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security; Beijing, China. 1755734: ACM; 2010. 337-340, DOI: 10.1145/1755688.1755734.

[21] Ibriq J, Mahgoub I. HIKES: Hierarchical key establishment scheme for wireless sensor networks. *International Journal of Communication Systems*. 2012:1-32, DOI: 10.1002/dac.2438.

[22] Bala Krishna M, Doja MN. Analysis of tree-based multicast routing in wireless sensor networks with varying network metrics. *International Journal of Communication Systems*. 2012:1-14, DOI: 10.1002/dac.1400.

[23] Simplicio MA, Sakuragui RRM. Cryptanalysis of an efficient three-party password-based key exchange scheme. *International Journal of Communication Systems*. 2012; 25(11):1443-1449, DOI: 10.1002/dac.1373.