International Journal of Security and Its Applications
Vol. 13, No. 4 (2019), pp.101-116
http://dx.doi.org/10.33832/ijsia.2019.13.4.10

LTA: A LINKED TIMESTAMP BASED AUTHENTICATION PROTOCOL FOR SENSOR NETWORK

Amit Kumar Gautam[1*] and Rakesh Kumar[2]

[1,2]*Madan Mohan Malaviya University of Technology, Gorakhpur, India*
[1]gautam.biet@gmail.com, [2]rkiitr@gmail.com

***Abstract*— Wireless Sensor Networks (WSNs) comprised of numerous spatially scattered autonomous devices that receive and transmit data using an insecure wireless channel. A sensor network is one of key development technology for IoT standards. It enables cooperation of heterogeneous information among devices and services. Security in wireless communication is a major concern not only for authenticated sources but also for transfer consistent data from sender nodes to base station while maintains network obtainability. Linked timestamping generates hashed timestamps, which is hooked on prior timestamps in authentic way. A slight change in timestamps value cancels the linked timestamps block. The serial order of linked timestamps is also saved by making backdating of the issued timestamp. The proposed method uses hashed linked timestamp authentication and is based on current timestamp in which information is encrypted with strong public-key cryptography for every sensor node. Therefore, it makes feasible to defend against various active and passive attacks. Complexity analysis has been done to show the superiority of the proposed approach.**

***Keywords*— Wireless Security, Timestamps, Authentication, linking, Public-key cryptography, Hashing, Security Attacks**

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are a key technology in the twentieth century because of its compact size, cheap, and facility to work in remote hostile locations. WSN is an essential part of the Internet of Things (IoT), which is emerging in quickening speed. A number of new growths and various applications of wireless communications are published [1]. The Scholars and predictions have confidence in that WSN can make abilities for various areas such as home automation. Healthcare, nuclear power plant, agriculture, and Internet of Things. The forecast by IDTechEx about IP-addressed sensor device that it has growth $48 billion in 2025 from $0.68 billion in 2015, the forty-seven percent gross yearly increasing rate as shown in Figure 1. By 2020 the internet connecting device has more than 50 billion predicted by Cisco system. The internet connecting devices have included numerous sensors (i.e. heat, pressure, moisture, radiation sensors), IoT devices, actuators, smoke, gas, surveillance equipment, and many communication devices. As the growth rate of connecting devices increases the data is also bounces in exponential manner. More data need more security and always vulnerable to security attacks.

WSN has various challenges rather than wired networks. There are many constraints such as resource utilization, scalability of wireless network, broadcast communication,

Received: September 16, 2019
Reviewed: November 18, 2019
Accepted: December 4, 2019

ISSN: 2207-9629 IJSIA

distribution in an unattainable, unreachable remote area, and topology are major issues that need a protected solution [2]. As the usage of WSN rises rapidly from small sensor devices to bigger manufacturing industries, the security threats on various devices will also increase proportionally. Recently the internet networks are affected by many problems for name servers by botnet attacks. Some corporations like IoT devices developers can withdraw all the product which are affected by botnet. So, all smart IoT devices and other wireless communicating devices that are small part of the user's life to large oceans are constantly vulnerable to security threats [3]. The wireless network security is necessary for transmitting the trustworthy and trustworthy data from communicating devices to far base station but also for maintaining the scalability and reliability of network. We must sure that transferred data is transmitted by a sender node to the destination node. We need to design security solution for WSN which maintain the confidentiality when various security attack occurs during transfer of data among the node of WSN. Thus, the information and data are usable inside the network when network is under attack [4].

The companies which provide network security service have good opportunity to provide security service for smart devices. IBM provide security services by their product called IoT solutions practice which provides security services in one package. IBM also provides a security solution called Watson IoT, which merge number of API, which provides many security services viz. authentication, scanning, blockchain technology, key management [5][6]. The security in sensor networks has time, which has used in many cryptographic protocols. With the help of timing attack, the adversary can break many secure protocols viz. RSA and Diffie-Hellman.

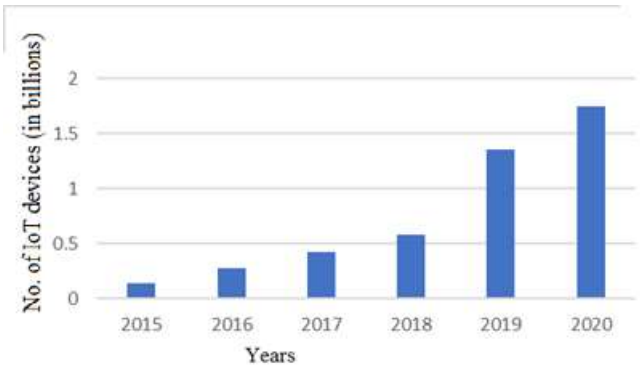

Fig. 1 Communicating devices predicted by IDTechEx [2]

1.1. AUTHENTICATION

Authentication is important criterion to secure WSN. It is an assurance that data comes from a genuine, honest and secure source. In the authentication procedure of wireless network any sender node Ns proves the receiver node N_r that it is N_s, and no other node proves to N_r that it is N_s. The sender node and receiver node called as prover and verifier respectively. The prover needs to authenticate to verifier that it is honest node and has valid cryptographic elements [4].

There are four kinds of authentication scheme in WSN, which are shown in Figure 2.

i. **Single (one) way Authentication**: The source node authenticates itself by one-sided single message to the receiver node. This single message holds sufficient information to verify that it is a legitimate user. One-way approach suffers from one drawback that the receiver node cannot give acknowledgment to the sender node.

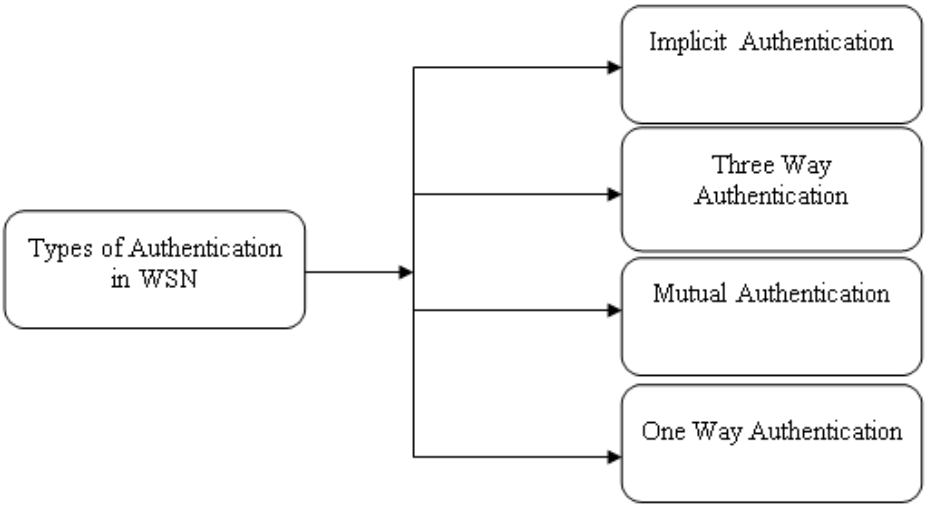

Fig. 2 Types of authentication in WSN

ii. **Two-way authentication**: This is a type of mutual authentication where the prover and verifier node authenticate each other. The certificate-based and the user name – password-based are the effective mutual authentication scheme.

iii. **Three-way authentication**: This type of authentication scheme has agreed to the involvement of third-party for authentication in WSN. The third-party verifies to both the sender and receiver by issuing an authentication certificate.

iv. **Implicit authentication**: Key management is used to authenticate the sender node. Implicit authentication scheme can reduce the computational overhead and energy reduction.

1.2. INSPIRATION, CONTRIBUTION AND ORGANIZATION

Our main motivation to develop a security solution based on timestamp issued by the node, which offers enhancement in authentication, safety, reliability, trustworthiness, and scalability to WSN placed in hostile and unattainable places. Our proposed linked timestamp-based method, which is not dependent on localized synchronized and unsynchronized clock. The previously proposed timestamp-based authentication schemes have some deficiencies like inability to protect from various types of malicious attacks and performance, efficiency, and computational overhead is good.

The sensors used in WSN are small, cheap cost, easily deployable, and small, which have limited memory, power, and processing devices. The broadcast, mobile, and wireless nature of sensors which make visible and attract many attackers. The absence of standard quantity of information, heterogeneity, environment and hard weight protection are major issues for WSN security. Fulfilling the authentication requirements also a key challenge. The major finding of proposed scheme are as follows:

- Comparison and analysis of various previously proposed authentication protocols.
- Proposed a linked hashed timestamp authentication technique to ensure integrity and validity.
- Analysis of performance and security on the basis of parameters correctness and feasibility of proposed linked hashed timestamp authentication scheme.
- We prove that the proposed authentication scheme offers defense and safety from various active and passive attacks.

The rest of this paper is organized as follows. Section 2 presented the background. Section 3 gives a related work and summarize the various works in the area of the authentication in WSN. The proposed method of linked timestamp-based authentication and provide security and performance analysis are presented in Section 4. Finally, the concluding remarks and future research directions are presented in Section 5.

2. BACKGROUND

2.1. TIMESTAMP BASED AUTHENTICATION PROTOCOLS

The protocol, which is using timestamp for authentication and validates the sender node, comes under the category of timestamp-based authentication protocol. The sender node is verified by the receiver node through calculating the valid time difference between timestamps. Therefore, the time difference is the key element to work this protocol.

The working of this protocol is like any node publishes a riddle and broadcasts. So, the honest node can solve this riddle is an acceptable amount of time, and the dishonest node solved this riddle in an unacceptable amount of time. In communication networks and public-key cryptography uses the Merkle's puzzle and calculate the quadratic difference between honest and dishonest nodes.

2.2. LINKED TIMESTAMPING

Suppose there are n sensor nodes between source and a destination node in WSN. All the nodes excluding the receiver node can generate timestamp, which is linked with a previously generated timestamp. So, the structure of linked timestamps is either a tree or chain structure, and it is validated at every level of structure. Similarly, like any storybook have many pages. Each page is synchronized with the previous page. If any page is missing, then the next page is not present the meaningful content. So, if anyone altered the content of the page then that page is easily identifying and invalidated [7].

Here every node generates a timestamp and takes the previous timestamp and hashed together to produce a bundle, and this whole hashed bundle is broadcasted in the network. If any attacker node wants to change a single bit of message, then the hash value of bundle is also change and impossible to find the preimage of that message. So, it is not possible to validate that block by the receiver node.

The following are the advantages of using linked timestamps.

i. The main advantage of using linked timestamping is that it does not need any cryptographic keys. So, no need to worry about losing cryptographic keys.

ii. The linked timestamping is faster and memory-efficient than other authentication schemes.

iii. The linked timestamp authentication schemes support scalability; therefore, it can efficiently deal with large and dense environments.

The following are the functionality provided by linked timestamps for authentication.

- **Aggregation of timestamps:** Timestamp based authority must combine all timestamps which are requested and not considered temporal and assigned time value.
- **Publication of timestamps:** When any node generates timestamps value, then timestamp authority publishes timestamps and also periodically updated, which will verifiable at any time.

- **Linked all timestamps:** The Merkle tree-based linking scheme is used to link all the timestamps. Each node produces a block which is hash value. Each block calculated with the hash value of previous timestamp and current timestamp value.

The following are the various evaluation parameters for authentication schemes.

- **Source Validation:** The main purpose of any authenticated protocol is to validate the sender node that it is a legitimate node. Every protocol has to positively deal with static and dynamic authentication.
- **Synchronize:** The time must be synchronized among all nodes in WSN. Each node must verify the previous timestamp without revealing any content of the block.
- **Computing Cost:** It is calculated by summation of all operations performed during generating and linking timestamps. These operations must include multiplication, hash operation, additions, and cryptographic operations.
- **Communication complexity:** It is evaluated as the aggregation of total cost during transmission and receiving the message with the total cost of unicast messages — the number of nodes updates such as the addition or deletion of any node from the network.
- **Integrity:** Integrity is the properties where it provides guarantees that the message would not change during the transmission.

2.3 BLOCKCHAIN BASED SECURITY

Blockchain is an innovative concept for security, which made an impact on secure transactions, wireless security, IoT security, distributed system, and many other life-changing uses. Zyskind et al. [8] give a method that focuses on blockchain technology to provide security, privacy of personal data, transactions and large volume of data. The linked timestamp-based approach is integral part of secure transactions as presented in Bitcoin.

In WSN, the timestamp-based protocol provides protection and defense against various security attacks. The linked timestamp comes with lightweight solutions in resource limitation WSN. Blockchain solution for decentralized cash system in electronic peer to peer networks was proposed by Nakamoto et al. [28]. It gives a new opening and opportunity to save a secure economic transaction. It is integrated part of scheme which can verify and validate block of distributed transaction. Every block is linked with hash function in Blockchain. This is linear data structure that is linked sequentially. Every block is linked with the previously hashed block with current to ensure the uniformity and immutability. To link all the block or transaction by using Merkle tree structure. Merkle tree has a root that has not changed during the transaction. if it is changed then the root of Merkle tree must be changed. During construction of Merkle tree, the tree can be forked from each node, but it considers longest chain in the network as safer [24].

3. RELATED WORK

There are various kinds of authentication schemes that take less communication overhead, reduce calculation load, reduce energy dissipation, resource consumption efficiently, such as storage, bandwidth, and power. Various lightweight authentication approaches are proposed by researchers. The authentication approaches are light by using a trust, elliptic curve cryptography, XOR operation, hash, and forward secrecy. Various types of authentication schemes are depicted in Figure 3.

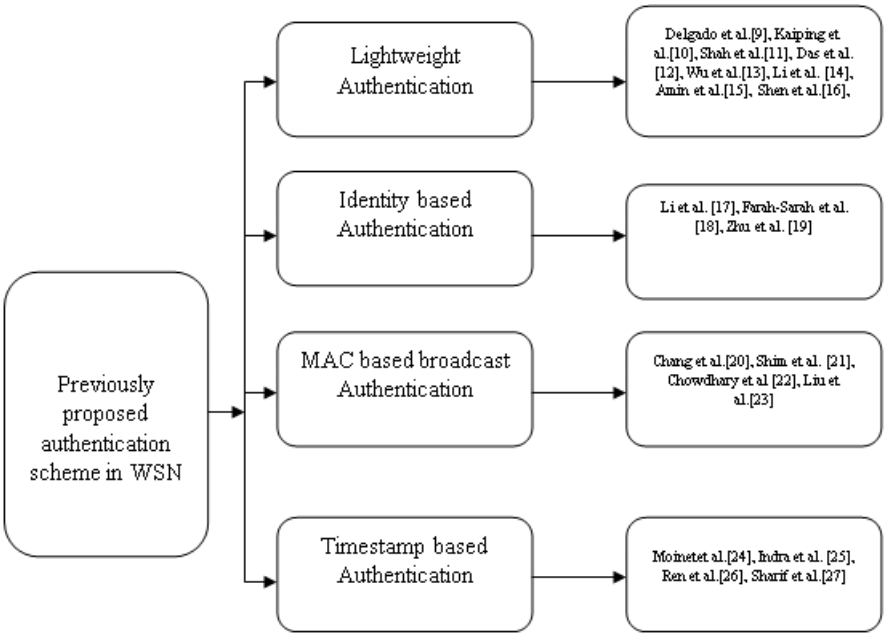

Fig. 3 Previously proposed authentication schemes in WSN

3.1. LIGHTWEIGHT AUTHENTICATION SCHEME

The lightweight authentication scheme mainly uses two-factor authentication. The advancement of two-factor authentication also proposed by some authors. Das et al.[12] have given authentication protocol which uses symmetric key cryptography and three-factor primitives. Wu et al. [13] recover the disadvantages and drawbacks in the method proposed by Das et al. [12] and provides an improved form of their approach. Li et al. [14] proposed an authentication scheme uses biometrics-based hashing called biohashing to improvised the security of three-factor authentication scheme. Jiang et al. [28] had identified drawbacks in existing three-factor security schemes. To overcome the drawbacks from previously proposed scheme he had given an authentication scheme based on Rabin cryptology. The specific attribute of Rabin cryptology is computational irregularity. By using fuzzy verifier, it can verify and validate the native password. This authentication scheme can protect the system against various internal and external attacks and use timestamps to protect from session-based attacks. A broadcast authentication scheme and data retrieval free services proposed by Kyung et al.[10]. This proposed method called BASIS, which had used identity-based authentication and also the combination of MRI-IBS and PMR-IBS. This method implemented a WSN scenario where MICAz and Tmote Sky are the sensors. They perform various experiments and found that this authentication scheme minimizes the memory overhead and computation complexity.

Kaiping et al. [29] find out the importance of the gateway node for security in wireless networks because all the traffic passes through the gateway node in both ways. The author proposed a two-way authentication approach by using temporal identifications. The password-based authentication method is used in this approach where the gateway node assigns some credit value to all nodes. After that the credit value attached to the identity of the user and stored in a card. The approach is lightweight and high protection because of using XOR and hash processes to reduce the complexity of the authentication approach.

Table I. Summary of lightweight authentication schemes

Previously proposed approach	**Publication year**	**Methodology used**	**Communication overhead**	**Advantage and disadvantages**
Kyung et al. [10]	2007	ID-based signature	4 TH + 4.5TS	Minimizes complexity and communication costs
Xue et al.[30]	2013	Temporal credential information	22 TH	Provides design of decentralized network but fails to provide satisfactory security
Shah et al. [30]	2014	Fermat Number Transform (FNT) and Chinese Remainder Theorem (CRT)	------	Defense against Cloning attack, Replay attack, DoS attack, and Man-in-the-middle attack. More complex scheme.
Das et al. [12]	2016	Biometrics information and smart card	25 TH	Energy-efficient method but does not provide scalability
Wu et al. [13]	2016	Biometrics information helps to register the user and sensor node	24 TH + 4TECM	Provides defense against spoofing, stolen smart card, and stolen verifier but cannot provide user anonymity.
Li et al. [14]	2016	Biohashing	18 TH + TS	Provide security against insider and node capture attacks. It does not provide user intractability
Amin et al. [15]	2016	Bio-hashing function	32 TH	Provides defense against the known security attacks. Not actually suitable for practical deployment.
Shen et al [16]	2016	Group key establishment algorithm between personal digital assistance (PDA)	6M+2H	Key escrow resilience, Non-reputation and key secrecy
Jiang et al. [28]	2017	Rabin cryptosystem	25 TH + TM+TQR	Secured approach but complex methodology

Delgado et al. [9] provide a lightweight encryption and decryption algorithm to authenticate any honest node in WSN. The proposed approach consumes less energy and communication cost. Shen et al. [16] proposed a source authentication of the source node in the wireless healthcare network. This protocol has castoff one to many and non-coupled authentication protocols approach that give confrontation against several security threats. The following Table I represented summery of lightweight authentication schemes.

3.2. IDENTITY-BASED AUTHENTICATION

In this scheme which uses identity as key element provide defense against various security threats in mobile ad hoc network, vehicular network, grid network, smart card, and different WSN applications. This type of protocol supports to create a secure, reliable, scalable, resource proficient, low computation, and suitable protocol for WSN. The summary of these authentication schemes is depicted in Table II.

Li et al. [17] proposed an authentication scheme that uses certificate-less public key cryptography. In this paper, the author points out some problems related to ID-based authentication such as key escrow problems and problem-related to certification. These problems can detect and solved by using conditional preserving authenticity. Therefore, this authentication scheme provides resilient against many security threats. Farah S. et al. [18] provides secure authentication among base stations and all sensor nodes. This scheme has used in a cluster-based sensor network where a central node is a cluster head and other nodes called cluster members. So, all cluster members have identity, and in their public key the identity plays an essential role. The public key drive from the identity of the nodes. The energy consumes during certification, and identity-based authentication is same. This protocol works in two-part. The first part deals with the delivery of private keys and in second step transferring of data securely.

Another ID-based signature scheme is proposed by Zhu et al. [19], which uses number theorem research unit lattice. It also uses the rejection sampling method instead of the general trapdoor.

Table II. Summary of identity-based authentication schemes

Previously proposed approach	Publication year	Methodology used	Communication overhead	Advantage and disadvantages
Mutual authentication scheme	2011	Elliptic curve cryptography	$3T_n+4T_h+4T_x+2T_m+10T_{MC}$	Prevents from active and passive attacks. Heavy method.
Farah S. et al. [18]	2016	Markov chain model	---	Drops selfish and denial-of-service attacks. providing effective security
Li et al. [17]	2018	Certificateless public key cryptography	$T = 2T_h + 3T_{epa} + 3T_{epm}$	Provides a faulty node detection and warning mechanism
Zhu et al. [19]	2018	Rejection sampling method	----	Protection against random oracle attack and quantum computer attack

3.3. BROADCAST AUTHENTICATION

The broadcast approach is beneficial in isolated and inaccessible fields. This approach must fulfill the evaluation criteria such as low computation overhead, instant verification, time synchronize, and defense against several security threats. The summary of the previously proposed broadcast authentication scheme is depicted in Table III.

On the basis of broadcast authentication generation, it has mainly two categories, first is signature-based and μTesla based authentication. A signature-based broadcast authentication scheme establishes asymmetric properties by using crypto primitives. There are some issues identified by Chang et al. [20] which are as follows:

- Using the large key size

- In some broadcast authentication schemes only, few messages are authenticated not all messages.

It authenticated the messages by issuing public and private keys by using their personal information. The cryptographic keys are generated and verified. This approach has many benefits over an earlier approach, like reducing the number of buffers, synchronization of time, and instant authentication. Shim et al. [21] proposed an authentication scheme called an efficient identity-based broadcast authentication scheme (EIBAS) for huge density of nodes and not mobile base station. This scheme has four stages: first system initialization, second private key mining, third creation of signature, and fourth broadcast authentication. The random number and hash function are used to create prime generator, and current timestamp is used to generate the signature. After that broadcast that message so, every node can verify that message. Chowdhary et al. [22] use a one-way hash algorithm for authentication called A lightweight one-way cryptographic hash algorithm (LOCHA). First convert the normal message in ASCII form then it breaks the message in packets of size 512. This packet again breaks and nested of size 8 bit, 64 bits 128 bits and 256 bits. Therefore, by swapping and transforming among levels it maintains uniformity and minimizes storage and communication overhead. Another broadcast authentication technique [23] uses signature approach to validate messages which are broadcasted. Consider k block of message, each block can authenticate by previous block authenticator, and only one signature can verify k messages. No time synchronization is needed.

Table III. Summary of broadcast authentication schemes

Previously proposed approach	**Publication year**	**Methodology used**	**Communication overhead**	**Advantage and disadvantages**
Chang et al. [20]	2006	pairwise symmetric keys which include with public and private information	----	Individual message authentication, removes buffer and time synchronization
Shim et al. [21]	2013	pairing-optimal identity-based signature	1P + 1E + 1M + 3H + 1SR	Shortest broadcast message size and improved energy efficiency 48.5% compared to other schemes
Chowdhary et al. [22]	2014	Multilevel ASCII codes	2952 X 9.4464μJ	preimage resistance, collision resistance
Liu. et al. [23]	2016	Signature amortization	----	Does not require time synchronization, authentication

3.4. TIMESTAMP BASED AUTHENTICATION

Linked chained authentication technique used by Moinet et al. [24] provides trust-based security in WSN. Here the combination of load and header is used as a block. The load is generated by the authority when any sensor node is added in the group. These payloads contain the public key and cryptographic information. So, the credential payload helps to verify that the block is valid. Here the problem is that it can contain only initial information to calculate the trust-based score. Gaurav et al. [25] have given a timestamp-based authentication key using ECC to validate the message. It is a mutual authentication

scheme that uses time synchronization. The ECC is lightweight, fast and contented with the dense environment. This approach efficiently manages the session and provide defense against many external and internal attacks.

Ren et al. [26] proposed two security methods, first based on the Bloom Filters and second called Hybrid Certification Scheme (HAS). This scheme certifies the nodes of WSN by using the Merkle tree. A public key and signature are used to generate a certificate by Certificate Authority (CA) for any sensor node. Cryptographic keys are also grouping of identification (ID) and authentication certificate of any node. After broadcasting they use flooding and authenticate the incoming message. Sharif et al. [27] proposed an authentication scheme for nodes that reduces cryptographic keys by using regeneration of keys. This scheme runs over another scheme. This can reduce complexity and supports scalable network.

4. PROPOSED TIMESTAMP BASED AUTHENTICATION APPROACH

Mutual agreed key generation

The basic idea behind our approach is that any new node wants to join the cluster with help other nodes in the cluster. The node generates a secure id for a new node in the network by forwarding their request to the cluster head.

Initialization Phase

Assume that there is a group (GP) of large prime number of order P, and G is the primitive element of G_P. The parameters G and G_P is available for all the nodes in the network. We had to calculate the public and private keys between sensor node N_A and N_B. Node N_A and N_B, which are already existing in the cluster, then both have chosen the PR_A and PR_B as their private key, respectively, and which belongs to G_P. The public keys of N_A and N_B are calculated as follows:

$$PU_{sn} = PR_{sn} \cdot G \quad \text{and} \quad PU_{ch} = PR_{ch} \cdot G$$

Mutual agreed key generation and exchange

1. Initially, node N_a selects a prime number G of order P and G_p and selects a random number R_a . After that node N_a computes $K_a = R_a \cdot G$ and sends the value of K_a to the node N_b .
2. After receiving the value of K_a the node N_b selects a random number R_b and evaluates $K_b = R_b \cdot G$ and sends the value of K_b to node N_a .
3. (i) After that receiving K_b by node N_a it computes $L_a = K_b \cdot R_a$
   (ii) The node N_b computes $L_b = K_a \cdot R_b$
   (iii) After that, calculates $L = K_a \cdot K_b \cdot G$, which is used as a secret mutual agreed key between node N_a and node N_b .
4. Now the public key of node N_a is R_a and private key K_a, and the public key of node N_b is R_b and private key K_b .

Timestamp generation

1. Consider sender node N_s which have private key K_s, and R_s is public-key want to send the message to receiver node N_r which have private key K_r, and R_r is public key through mediator node N_m.
2. First, with the help of key encrypt the message and node N_s then takes the value of T_j by calculating the current time from its local clock.
3. After that, calculate the linked timestamp. If N_s is the first node then the previous timestamp $T_{prev} = 0$ otherwise T_{prev} have some hash value.

4. Compute the linked timestamp

   $T_s = H (ID_s || T_{prev} || T_j)$

   Where ID_s is the identity id of current node id.

5. Broadcasts the T_s value.

Endorsement Phase

After getting the message of timestamp by receiver node N_r it verifies any point of communication. It calculates the current hash value of timestamp by using the previous timestamp. If it is equal, then it confirms that the message comes from an authenticated source otherwise discarded the message. Figure 4 depicted the schematic diagram of our proposed approach.

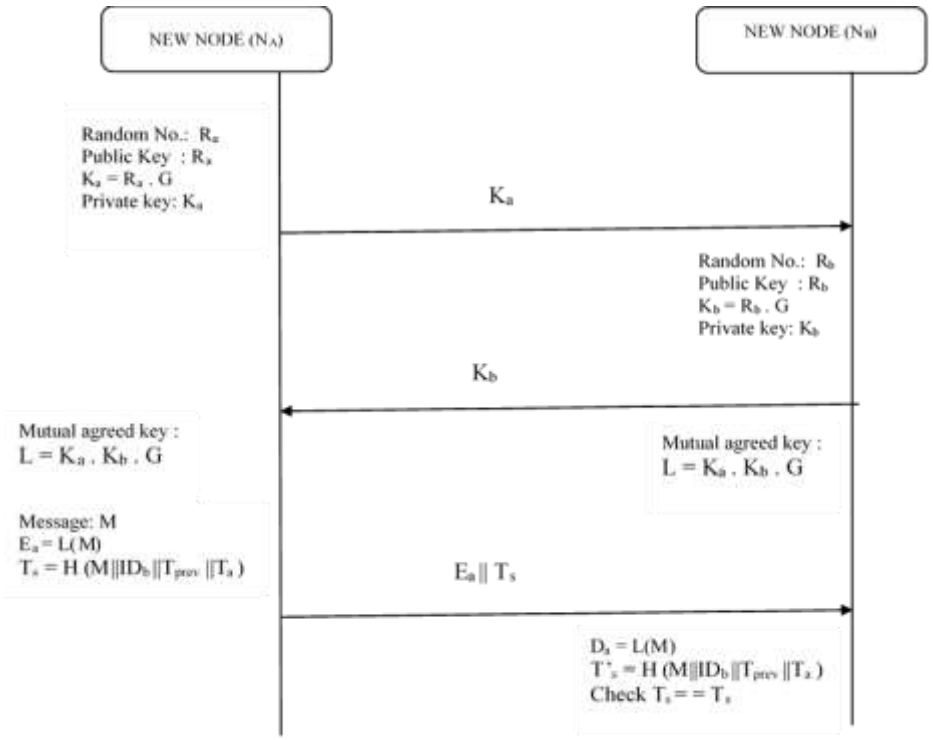

Fig. 4 Schematic view of proposed scheme

4.1. SECURITY ANALYSIS

- **Source authentication:** The LTA schemes provide assurance to the authenticity of the source node. Each receiver node can verify the source by calculating the hash value of linked messages with the publicly cryptographic chain value. The message is also encrypted with the cryptographic keys, so it is very hard to alter the message by any adversary. Suppose due to any circumstances can change a single bit of message then the hash value will totally different, and it could not be verified by the receiver node. Therefore, in our LTA scheme, the source authentication is guaranteed.

- **DoS attack:** Denial of Service (DoS) attack is a security threat that causes a reduction of memory capacity, blockage of various services, and supports other security threats. Here its LTA scheme no sensor node uses buffer to store authentication messages, and it immediately broadcast the authentic message without any delay. Therefore, the faulty packet injection and broadcasting

repeatedly are difficult. There is one disadvantage that drain of battery is higher, but it could be reduced by limiting the false authentication

- **Passive Attacks:** Passive attackers can sniff the traffic between nodes and take cryptographic information such as patterns, and the nature of traffic can be used against the network. This type of attack can be counter by using strong cryptographic keys. And the authentication message is strongly hashed so it is impossible to break and find the preimage of hashed data.

- **Sinkhole attack:** Sinkhole attack is the main attack in WSN, where it attracts all the traffic towards the adversaries. The sinkhole node receives all the packets and discards it. Here the malicious node behaves like a sink node and attracts all communication towards it. The LTA scheme uses hashed timestamp, which is linked with the hash function are strong defense against the sinkhole attack. The verification of source node is by strong public-key cryptographic approach. The same hash value is not generated by an adversary. Therefore, the proposed LTA scheme can protect from sinkhole attack.

- **Wormhole attack:** Wormhole attack, where adversary's node strategically placed in the network. It is placed at a different end of the network and coordinates with individual node to usage low latency side channel for communication in WSN. So, messages are bypass all other nodes and pass-through tunnel. The proposed LTA based scheme offers protection against wormhole attack. LTA scheme checks timestamp variance at the receiver end. If the variance is larger than the datum value, then it directly ends the session and reports the node is malicious. Therefore, the proposed LTA scheme successfully defend (defense) against the wormhole attack.

- **Node Compromised Attacks:** The nodes are physically attacked and capture information stored in it. The attacker can compromise the node's information, such as cryptographic keys, identity, and other relevant information. The LTA schemes used current timestamp and data are encoded with strong public-key cryptography. So, it made achievable to protection against the diversity of node capture attacks.

- **Real-time Attacks:** The dynamic attackers have more capability to harm the network in wireless channels. The adversary node can modify data, routing attacks, node capture attack, noise and intercept communication. The real-time attack can be prohibited by the LTA scheme by generating real-time dynamic timestamps and other parameters at every session. Therefore, it can protect the networks by all the real-time attacks.

4.2. PERFORMANCE ANALYSIS

Linked timestamping is quicker than simple public-key cryptography deprived of special cryptographic hardware. In linked timestamping no need to worry about cryptographic key-related risk. Therefore, the timestamp value is guaranteed for lifelong. Because of the hash function, timestamp life timestamp is longer than public key signature scheme. The proposed LTA scheme strong public-key cryptography and use for the public key and private key, which valued the computation cost between any node and base station is 5578.2 ms for a specific session and 36476 ms for 1024-bit RSA. Compared to RSA scheme our LTA scheme performed better and reduced the computational cost of key generation in a session.

Table IV. Symbol table

Symbol	Definition
TH	Hash Computation Time
TPA	Elliptic Curve Point Addition Computation Time
TPM	Elliptic Curve Point Multiplication Computation Time
TE	Elliptic Curve Polynomial Computation Time
TPR	Private Key Computation Time
TPU	Public Key Computation Time

The performance analysis between the LTA scheme and previously existing scheme based on computation cost. Consider the following notation used for comparison. The computations complexity of the hash function is lesser than the public and private key calculation time, which means that TPU > TH and TPR > TH. The computation cost of public and private key generation is polynomial computation cost. But the computation complexity of TPA, TPM, and TE takes cubic polynomial time. The computation time of TH takes linear, and in the worst case, it takes quadratic time.

5. CONCLUSION AND FUTURE DIRECTIONS

In this work, we proposed a linked timestamp authentication mechanism for secure communication in a sensor network. Various recently proposed authentication techniques and the most advanced timestamp-based mechanisms in WSN are studied and summarized. So, in order to overcome the limits and restrictions, we have used public-key cryptography and linked timestamp-based authentication. The proposed linked timestamp-based authentication scheme has been designed and organized in a systematic way and combined different properties, which in turn depends on the security of the public keys such as two-way key generation, timestamp generation, and linking and timestamp verification. The proposed scheme offers the highest cryptographic strength per bit among all existing public-key cryptosystems. It also helps the sender node, which promises to provide defense against security threats to the reliability and conformity of WSNs in a distributed environment.

Nevertheless, the same proposed linked timestamp-based authentication and key management scheme for a particular session in WSNs can be extended efficiently for a multi-session scenario in the domain of WSNs or in the IoT networks.

ACKNOWLEDGEMENT

This paper is funded by the University Grant Commission (UGC), India, under Junior Research Fellowship (UGC NET-JRF) vide letter no. 3331/(SC)(NET-JUNE2015).

REFERENCES

[1] Al-Rakhami, Mabrook, and Saleh Almowuena. "Wireless Sensor Networks Security: State of the Art." arXiv preprint arXiv:1808.05272 (2018)
[2] Grace, Roger. "Sensors to support the iot for infrastructure monitoring: Technology and applications for smart transport/smart buildings." Internet of Things Technology Symposium. 2015.
[3] Rouvala M. “White paper: Security and WSN”. New Nordic Engineering. November 2017.
[4] Rajeswari, S. Raja, and V. Seenivasagam. "Comparative study on various authentication protocols in wireless sensor networks." The Scientific World Journal 2016 (2016).

[5] Li, Yannan, Willy Susilo, Guomin Yang, Yong Yu, Dongxi Liu, and Mohsen Guizani. "A Blockchain-based Self-tallying Voting Scheme in Decentralized IoT." arXiv preprint arXiv:1902.03710 (2019).
[6] Jaiswal, Priyanka, and Sachin Tripathi. "An authenticated group key transfer protocol using elliptic curve cryptography." Peer-to-Peer Networking and Applications 10, no. 4 (2017): 857-864.
[7] Buldas, Ahto, Peeter Laud, Helger Lipmaa, and Jan Villemson. "Time-stamping with binary linking schemes." In Annual International Cryptology Conference, Springer, Berlin, Heidelberg, (1998) pp. 486-501.
[8] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In 2015 IEEE Security and Privacy Workshops, (2015) pp. 180-184. IEEE.
[9] Delgado-Mohatar, Oscar, Amparo Fúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks 9, no. 5 (2011): 727-735.
[10] Shim, Kyung-Ah. "BASIS: a practical multi-user broadcast authentication scheme in wireless sensor networks." IEEE Transactions on Information Forensics and Security 12, no. 7 (2017): 1545-1554.
[11] Shah, Manali D., Shrenik N. Gala, and Narendra M. Shekokar. "Lightweight authentication protocol used in wireless sensor network." In 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), (2014), pp. 138-143. IEEE
[12] Das, Ashok Kumar. "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks." Peer-to-peer Networking and Applications 9, no. 1 (2016): 223-244.
[13] Wu, Fan, Lili Xu, Saru Kumari, and Xiong Li. "An improved and provably secure three-factor user authentication scheme for wireless sensor networks." Peer-to-Peer Networking and Applications 11, no. 1 (2018): 1-20..
[14] Li, Xiong, Jianwei Niu, Saru Kumari, Junguo Liao, Wei Liang, and Muhammad Khurram Khan. "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity." Security and Communication Networks 9, no. 15 (2016): 2643-2655.
[15] Amin, Ruhul, SK Hafizul Islam, G. P. Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks." Computer Networks 101 (2016): 42-62..
[16] Shen, Jian, Shaohua Chang, Jun Shen, Qi Liu, and Xingming Sun. "A lightweight multi-layer authentication protocol for wireless body area networks." Future generation computer systems 78 (2018): 956-963..
[17] Li, Congcong, Xi Zhang, Haiping Wang, and Dongfeng Li. "An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks." Sensors 18, no. 1 (2018): 194.
[18] Ferrag, Mohamed Amine, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. "Authentication protocols for Internet of Things: A comprehensive survey." Security and Communication Networks 2017 (2017).
[19] Zhu, Hongfei, Yu-an Tan, Liehuang Zhu, Xianmin Wang, Quanxin Zhang, and Yuanzhang Li. "An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks." Sensors 18, no. 5 (2018): 1663.
[20] Chang, Shang-Ming, Shiuhpyng Shieh, Warren W. Lin, and Chih-Ming Hsieh. "An efficient broadcast authentication scheme in wireless sensor networks." In Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pp. 311-320. ACM, 2006.
[21] Shim, Kyung-Ah, Young-Ran Lee, and Cheol-Min Park. "EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks." Ad Hoc Networks 11, no. 1 (2013): 182-189.
[22] Chowdhury, Amrita Roy, Tanusree Chatterjee, and Sipra DasBit. "LOCHA: a light-weight one-way cryptographic hash algorithm for wireless sensor network." Procedia Computer Science 32 (2014): 497-504.
[23] Liu, Yongsheng, Jie Li, and Mohsen Guizani. "PKC based broadcast authentication using signature amortization for WSNs." IEEE Transactions on Wireless Communications 11, no. 6 (2012): 2106-2115.
[24] Moinet, Axel, Benoît Darties, and Jean-Luc Baril. "Blockchain based trust & authentication for decentralized sensor networks." arXiv preprint arXiv:1706.01730 (2017).
[25] Indra, Gaurav, and Renu Taneja. "A time stamp-based elliptic curve cryptosystem for wireless ad-hoc sensor networks." IJSSC 4, no. 1 (2014): 39-54.
[26] Ren, Yongjun, Yepeng Liu, Sai Ji, Arun Kumar Sangaiah, and Jin Wang. "Incentive mechanism of data storage based on blockchain for wireless sensor networks." Mobile Information Systems 2018 (2018)
[27] Sharifi, Mohsen, Saeed Sedighian Kashi, and Saeed Pourroostaei Ardakani. "Lap: A lightweight authentication protocol for smart dust wireless sensor networks." In 2009 International Symposium on Collaborative Technologies and Systems, pp. 258-265. IEEE, 2009.
[28] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[29] Jiang, Qi, Sherali Zeadally, Jianfeng Ma, and Debiao He. "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks." IEEE Access 5 (2017): 3376-3392.

[30] Xue, Kaiping, Changsha Ma, Peilin Hong, and Rong Ding. "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks." Journal of Network and Computer Applications 36, no. 1 (2013): 316-323.
[31] Shah, Manali D., Shrenik N. Gala, and Narendra M. Shekokar. "Lightweight authentication protocol used in wireless sensor network." In 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), pp. 138-143. IEEE, 2014.
[32] Luo, Hanguang, Guangjun Wen, and Jian Su. "Lightweight three factor scheme for real-time data access in wireless sensor networks." Wireless Networks (2018): 1-16
[33] Gope, Prosanta, and Tzonelih Hwang. "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks." IEEE Transactions on Industrial Electronics 63, no. 11 (2016): 7124-7132.

