A Lightweight Authentication Method in Perception Layer of IoT Through Digital Watermarking

Neeraj Kumar, Deepak Singh Tomar

Abstract: ***Introduction of IoT (Internet of Things) has enjoyed vigorous support from governments and research institutions around the world, and remarkable achievements have been obtained till date. IoT systems collect the voluminous amount of data in real time from hospitals, battlefield and daily living environment which is related to privacy and security of people. So, securing collected sensitive data is one of the major challenges in the development of IoT systems. Authenticating the source of collected data is utmost important because the adversary may act as a source which may lead to a breach in security and privacy of people using the IoT network. IoT devices are resource scarce so lightweight methods for network security and privacy need to develop to achieve future development goals. In this paper, a novel lightweight node to node authentication scheme based on watermark is proposed to solve the contradiction between the security and restricted resources of perception layer. To improve the security, Proposed scheme usage node identity and the number of neighbours as input to generate the watermark and use the watermark to calculate the embedding positions which makes node authentication based on temporal dynamics of sensing network. The generated watermark is embedded in fixed size message digest generated using the variable message as input into a low-cost one-way hashing algorithm LOCHA. The embedded bits of watermark extracted at the receiving node and matched to check the authenticity of the sender node. The security analysis and simulations of the proposed scheme show that it can be a good candidate to ensure the authentication of the resource constraint devices which are integral part of Internet of Things at low cost.***

Index Terms: Authentication., IoT(Internet of Things), LOCHA, Watermark,

I. INTRODUCTION

IoT is a collection of physical things (e.g. sensors and actuators) with limited battery and computational power is an emerging service infrastructure and network environment. Physical objects are basically the collection of actuators sensors, tags or mobile devices used to collect real-time data from Smart homes, Healthcare, Traffic, Industry, Agriculture and Breeding, Pharmaceutical industry, etc. The architecture of IoT comprises of things layer (Perception layer), Network layer and Application layer [2]. Things layer is basically a hardware layer consisting of sensors and actuators which are basic components of the IoT environment. Network layer and application layer of IoT deals with existing mature technology which is capable of secure handling of data.

Perception layer deals with emerging technology which is Resource constraint, Low power and in its immature phase used to percept information from the Physical world. Perception data is very sensitive so disclosure of it is a great cause of concern for IoT development. Perception layer of IoT is functionally identical to WSN.

This paper talks about the node authentication in the transmission of perceived data. Battery power, dynamics of nodes, limited processing and storage are major challenges in Node authentication in the perception layer. Perception layer is vulnerable to replay attack a kind of DoS attack if node authentication fails and if the node authentication mechanism breached somehow then the perception layer is also prone to masquerade attack. Node authentication is one of the security challenges in the development of IoT because the security of IoT systems is utmost important.

Traditional network usage Message Authentication Codes (MAC) and Cryptography for authentication purpose. To support encryption and decryption Complex computation and extra space to store keys are required which leads to a burden on resource constraint sensor nodes [3]. Digital watermarking Technologies proposed as an efficient protection scheme for authentication of nodes in the perception layer. Digital watermarking widely used to protect content integrity and copyright information of digital multimedia (video, audio, and images, etc.) [4]. Digital watermarking is faster than encryption technology requires less computing power, less overhead of storage and bandwidth provides better security and cryptography [5].

According to literature digital watermarking can be done in two types i.e. Robust watermarking and Fragile watermarking [6]. Robust watermarking is used for copyright protection and Fragile watermarking may be used for authentication purpose so it can be used for authentication of nodes in perception layer of IoT. In this paper, Fragile digital watermarking is proposed and developed for Node authentication in the perception layer of IoT.

Revised Manuscript Received on September 25, 2019.

Neeraj Kumar, Computer Science and Engineering Department, Assistant Professor, Shri Ramswaroop Memorial University Lucknow, India. Email: neer1990@gmail.com

Dr. Deepak Singh Tomar, Computer Science and Engineering Department, Associate Professor, Maulana Azad National Institute of Technology, Bhopal, India.
Email: deepaktomarmanit@gmail.com

II. RELATED WORK AND NEED FOR AUTHENTICATION IN IOT DEVICES

A. Related work

Perception layer of IoT architecture is in its immature phase of development. Now a day's researchers are focused to strengthen the security of physical objects in perception layer to prevent the harmful attack which may lead to major consequences for whole IoT ecosystem.

In this paper Node to node authentication in the perception layer (WSN) is discussed. Some of the Node authentication mechanism for the perception layer discussed so far are as follows.

Li and Song [7] propose a trust scheme for the vehicular ad hoc networks (VANETs) to protect collected data and the node in the VANETs. The proposed model can appraise the trustworthiness of the data and the nodes, respectively. What is more, it can also locate the malicious node in the VANETs and own resistance to a variety of attacks.

LEAP [8] is a key management protocol is proposed for radio sensor networks for preventing the impact on neighboring nodes due to the injection of the malicious node and to support in-network processing. However, Scheme requires high computation and communication overhead and significant memory for key storage so the scheme is not supposed to be a good candidate for implementation in resource-scarce IoT sensor environments.

Adrian Perrig et.al proposed Sensor Network Encryption Protocol (SNEP) [9] used for two-party authentication, confidentiality, freshness and Data integrity. Data is encrypted using a counter value encryption key. But encryption protocol leads to the addition of 8 bytes per message which is a huge overhead for power constrained sensor nodes. The sink node assumes source authentic for consecutive message If the next message has a higher counter value than previous. Management of Counter states needed a counter exchange protocol which leads to extra communication and computation overhead to the scheme.

Elliptical curve cryptography-based authentication protocol [10] is based on prevention of non-authentic nodes to join the WSN by making use of timestamp. Protocol-based on key establishment Phase to help the legitimate new nodes to share keys with their neighbors for the purpose of performing secure communication. This scheme is able to handle various attacks but on the cost of huge computation and communication overhead.

A Distributed node authentication scheme [11] based on latitude and longitude of sensor nodes. In this scheme, notes maintain a data set of distance between themselves and neighbors. If the security of any sensor node is breached the malicious node with duplicate identity is detected by calculating the change in distance and the base station is informed. This scheme provides good results for identity replication attack [12] but fails to provide protection against Sybil attack [13].

A decentralized authentication and key management scheme [14] used for Note authentication in WSN with the high hierarchical structure. The node authentication mechanism is highly efficient but mutual authentication and exchanging mechanism of key leads to high communication overhead. It works well for hierarchical structure but fails to incorporate the flat structure.

Arpan Sen et.al proposed a Low overhead watermark-based node authentication (LoWaNA) [15] to be used for Node authentication in unicast communication with flat architecture. Masquerade and replay attacks can be handled efficiently using LoWaNA. This scheme uses MD5 to calculate message digest which increases the computation overhead. Future research in LoWaNA could be to use any less computation intensive algorithm to calculate the hash digest which will enhance the performance of LoWaNA.

This kind of algorithm is easy to implement and has a low time complexity, which satisfies the requirements of highly resource-constrained WSNs to a certain extent. In order to solve these problems, this paper presents a lightweight watermarking technique. The proposed algorithm calculates the embedding position of watermark dynamically by based on sensor identity and the number of neighbors, which not only improves the security but also saves energy and realizes real-time node authentication.

B. Possible attacks on Perception layer of IoT

In this paper, the adversary model is considered similar used in [16]. The model has three types of attackers.

A passive attacker: An eavesdropper can keep watch on sensitive information being transmitted on the radio network.

An Internal attacker: This may compromise any internal node or cluster head physically.

An External attacker: This may modify or replay the data being transmitted. The external attacker can inject false data from outside. Various attacks can be launched by attackers described above based on their abilities.

Type 1: Attacker can launch an eavesdropping attack to sense the secret information.

(a) Eavesdropping attack: Passive attacker listens to secret messages being broadcasted in a wireless medium to extract information for the future attack.

Type 2: Attacker or Internal attacker can sense all secret parameters i.e. sensor Id, Timestamp, Location coordinates, etc. that may lead to compromised node attack.

(a) Node or Cluster Head compromise attack: Cluster head or sensor node can be compromised by an internal attacker to generate the secret parameters of the network.

Type 3: External attacker can transmit false data by altering the contents of packets, false packet injection and replaying the packets of earlier transmission. Three types of attacks can be launched by Type 3 attackers.

(a) Packet Tampering: Tampering of data packets can be done by an external attacker which may lead to serious consequences for security sensitive applications.

(b) Packet replay attack: Attacker forwards the packets which are already forwarded the lead to heavy network traffic and the waste of energy for energy and computation sensitive nodes.

(c) Packet forgery attack: Attacker injects fake packets which leads to heavy network traffic and the waste of energy for whole WSN.

C. Experiment setup

Analysis of the proposed scheme is done on Contiki [19] operating system with the help of cooja simulator which is a powerful simulation tool for perception layer devices in IoT. In Cooja an alternative protocol stack RIME [20] is used to reduce the overhead. RIME stack is low overhead communication protocol stack which is designed to suit with lousy networks is implemented in cooja so cooja emerges as a powerful simulation tool for IoT devices.

In the simulation, MICAz motes are used. In this paper 25 nodes are placed because of the system constraint of running independent program on all nodes placed across a 100 *100 m grid with the transmission range of each sensor is set to 55 with radio traffic interference range of 100 m for each node. Unit Disk Graph Model (UDGM) [27] is used as a radio. Sensed data can be unicasted to one hop neighbors present in any of the four directions so communication is assumed random in nature.

D. Proposed work

In this paper digital watermarking scheme is proposed for Node to Node authentication from type2(a) and type3(b) adversary given in section II. The fragile watermarking scheme is used to prevent adversary as it is sensitive to any modification. Once the data in transmission is modified the embedded watermark in data will be destroyed. Any adversary acting as legal node will not able to restore original data without knowledge of the watermarking scheme.

Any fake packets injected by adversary also be detected at the sink because fake packets may not be verified at the sink with the watermarking scheme.

The watermarking scheme consists of three phases namely watermark generation, watermark embedding, and watermark extraction as shown in figure1.

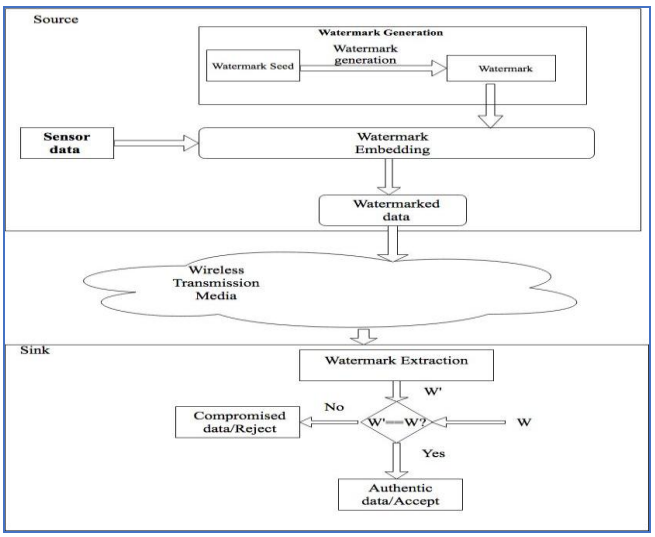

Figure 1: Working of Watermarking Scheme

Firstly, the watermark generation process takes encrypted sensor data as input and generate the watermark as output which will be embedded into data to be transmitted.

Secondly, the watermark embedding process takes sensed data and watermark generated for merging to form a new packet according to predefined rules for being transmitted.

During transmission, various types of attacks can happen as discussed in section III.

Thirdly, Watermark extraction takes place at the sink where the transmitted packet from source is received, watermark extraction takes place and original sensed data is restored according to extraction algorithm.

The same Watermark generation process is used to generate the watermark from the received data. To verify the node authenticity extracted and regenerated watermark are matched if they are same means node is authenticated else the node is compromised. The algorithm for the watermarking process is hidden to adversary so it is very difficult to generate and embed the watermark.

1) Algorithm

The proposed algorithm composed of three algorithms Watermark generator, Watermark embedder and Watermark extractor described as follows.

Inscription:

1. Hashed data size (bits): h
2. Generated Watermark length (bits): l(l<h)
3. Packet size (bits): h+2l

Each node consists of 3-tuple data:

1. Unique Identity (N_Id)
2. Number of adjacent nodes (No_of_adj)
3. Variable count initialized to 0

Each sensor node stores n-bit counter entries for all its adjacent sensors initially set to 0.

a) Watermark generator

Input: Sensor identification bits, number of neighbors
Output: generated w-bit watermark
Start

Step1: Extract l-bits from LSB of sensor identity and from number of neighbors if bits are less than n then padding is done in MSB with 0's to make n-bits .

Step2: Perform Ex-or on individual extracted bits taking sensor identity bits from MSB to LSB and Number of neighbor bits from LSB to MSB.

Step3: Result of Ex-or operation is an n-bit watermark.

End

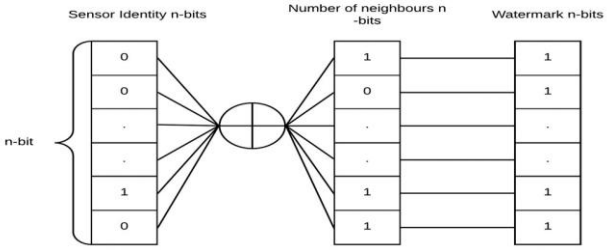

Figure 2: Watermark generation

b) Watermark Embedder

Input: Generated watermark (l bits), Counter (l bits) and message digest (h bits).
Output: Embedded message(h+2l) for transmission in radio network.
Start
Step1: Compute Modulo sum of watermark (0 or 1) store in variable q.
Step2: Finding the positions for embedding of watermark and counter bits. Positions are based on the value of q if q is 0 then placing q at MSB+1 position and if q is 1 then placing it at MSB in watermark and computing decimal value from binary formed which will be the position of inserting watermark bit and the counter bit next to it.
Step3: Insert one bit from MSB of watermark and counter at position and position+1 respectively.
Step3: Repeat step 2 and 3 for MSB to LSB in watermark and counter.
Step 4: Check for counter overflow if all bits are 1 then reset it to 0.
Step 5: Increment counter for next message transmission.
Step6: Break message digest into three parts. The number of bits in first and second fragment is decimal equivalent to first l bits from LSB of sensor identity and the number of neighbor's binary value computed in watermark generation algorithm and all remaining bits of embedded digest will form the third fragment.
Step 7: Return all three fragments for transmission
End

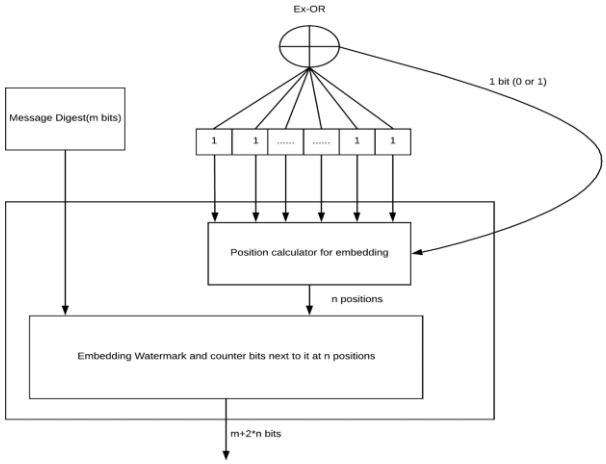

Figure 3: Watermark Embedding

c) Watermark extractor

Input: Received three fragments (First, Second, Third)
Output: Accept/Reject
Start
Step1: Find the length of First and Second.
Step2: Convert length of First and Second to a binary value.
Step3: If the bit lengths of First and Second is less than watermark length (l) then padding is done in MSB with 0 to make length l.
Step4: Calculate watermark using First and Second binary value with the help of **watermark generation procedure (a)**.
Step5: Find the positions of embedding using the generated watermark using step2 of **Watermark Embedding procedure (b)**.
Step6: Extract watermark and counter bit pair from embedded positions.
Step7: Compare generated watermark and computed watermark and counter value already stored with the receiving node.
Step8: If watermark matched and counters mismatch go to step 9 otherwise go to step 10.
Step9: Accept
Step10: Reject
End

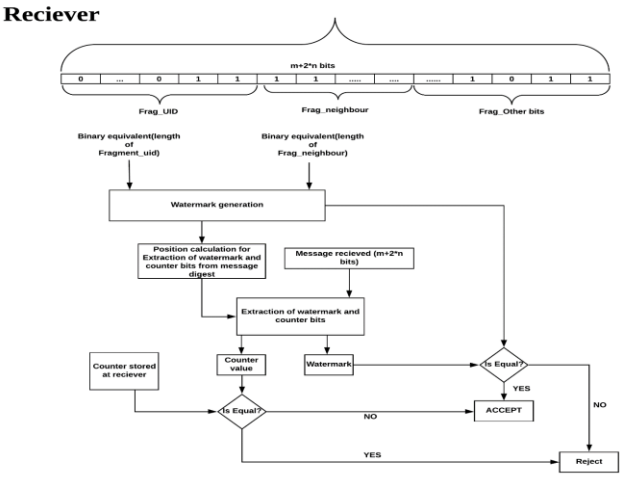

Figure 4: Watermark and Counter extraction and matching

III. RESULT ANALYSIS

A. The computational complexity of the proposed authentication method

The time complexity of watermark generation procedure (4.1.1) is O(w) where w bits are generated. Embedding of watermark (4.1.2) bit and counter bit requires O(d) time where d bits are generated by application of hashing on data and embedding of w bits to be done so total computational cost for embedding is O(d*w)+H where the H is time required for generation of message digest using LOCHA hashing algorithm. Watermark extraction (4.1.3) procedure requires O(d) time for one bit and w bits are to be extracted hence the time required is O(w*d). So each message being transmitted requires O(w*d)+H time. The time complexity of LOCHA is O(d)[1]. So Computational complexity of procedure will be O(d)+O(d*w)+O(d)+O(w*d) resulting to O(w*d).

B. Performance evaluation

The performance of the proposed method is evaluated qualitatively and comparatively.

1) Quantitative analysis

In Quantitative analysis, performance measurement is done using cracking probability and average cracking time.

a) Cracking probability

The probability of generating watermark and embedding positions of the watermark may be treated as one of the performance parameters for the proposed method.

An adversary may act as an authenticated node if watermark generation and embedding positions somehow decoded. The cracking probability can be calculated as follows.

Assume size of the watermark is w and the size of the digest is h then the total number of combination possible for watermarks is 2w and probability to generate the desired watermark is 1/2w.

The probability of calculating the desired position for watermark embedding in message digest is $\mathbf{1/{}^{h}P_{w}}$.

Hence cracking probability can be computed as $(1/2^{w})*(1/{}^{h}P_{w})$.

Cracking probability of proposed method with w=6 and message digest h=96 is $2.34*10^{12}$.

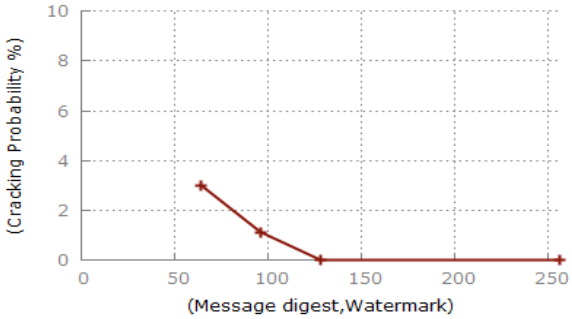

Figure 5: Cracking probability vs. Varying message length

b) Average cracking time

The time required by an adversary to generate the same message as the authentic node by application of Brute force method is cracking time. Cracking time for the proposed method should be greater than the network existence for the success of node authentication.

MICAz mote is taken as attacker node an average cracking time is calculated as follows.

The number of the trail for watermark generation is 2^{w} hence the average number of trails to get correct bits are 2^{w-1}.

Similarly, the average number of trails to find correct embedding positions are ${}^{h}P_{w}/2$.Hence the average number of trails for both generation and embedding are $2^{w-1}* {}^{h}P_{w}/2$. For w=6 and h=96 the average number of trails will be $1.06*10^{13}$.

Now considering the MICAz mote working at 16MHz and the clock required for embedding algorithm are

1000 then total clocks required $1.06*10^{13}*1000=1.06*10^{16}$.

The time required by the attacker to break the authentication using brute force = $1.06*10^{16}/16*10^{6}=6.62*10^{8}$sec or 22 years. The cracking probability and cracking time increase with the number of watermark bits and different length of hash digests.

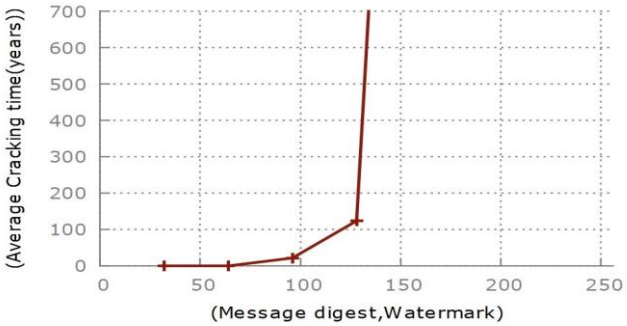

Figure 6: Average Cracking time vs. Varying message length

2) Comparative analysis

Comparative analysis is done on basis of communication overhead as it is well known that communication overhead is 3000 times of the computation overhead so if proposed method is better in communication overhead the performance of proposed method will be better. The comparison table1 is based on communication overhead given as follows.

Table 1: Communication overhead comparison

Scheme	Communication overhead(µj)	
	Transmission	Receiving
IBE trust + one-way AKE [17]	580.00	950.00
Watermark scheme [18]	92.40	103.18
LoWaNA[15]	84.40	93.80
Proposed Scheme	64.8	72.36

From the above table, the communication gain of the proposed scheme is 23.22 %, 22.85% in transmission and receiving respectively. This gain in communication significant in terms of energy for power constraint sensor in IoT. In this paper, simulation is performed in two scenarios. A sample run is done 40 times in each scenario. In the first case scenario, all nodes taken are authentic and messages received with 100% success rate as shown in fig a. The second scenario is simulated with a Sybil node for 40 times and it is observed that 4-5% message on average has been rejected which are assumed from Sybil node. Comparison between LoWaNA and proposed scheme is done for communication overhead which is major energy consuming part of the WSN network and proposed scheme comes to be superior over LoWaNA as shown in fig[5].

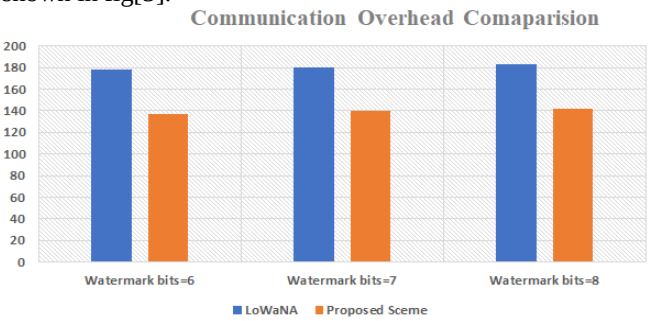

Figure 7: Communication overhead LoWaNa vs. Proposed scheme

IV. CONCLUSION

In this paper, a lightweight, energy efficient scheme for node authentication using digital watermarking method is proposed for securing the unicast hop to hop communication in Perception layer of IoT. To make scheme suitable for IoT node to node authentication the computing procedures are designed in the way to minimize computation and communication overhead with help of low-overhead operations like Ex-XOR, Embedding, Extraction of bits as much as possible. A Light-Weight One-way Cryptographic Hash Algorithm: LOCHA designed for resource constraint sensor nodes is used for calculation of the message digest used in process of authentication among sensor nodes.

Cracking probability is used to verify the computation hardness for the proposed scheme proves it over performing. Cracking time parameter used to check breaking time of security method prove the scheme safe for required durations.The scheme is compared with previously related schemes on the basis of communication overheads as the communication overhead is dominating performance parameter for IoT perception layer/Wireless sensor network confirms our scheme is over performing to all related proposed schemes in terms of communication overhead. Finally, the proposed scheme is compared with LoWaNa scheme using cooja simulator with mote e.g. MICAz. The LoWaNa scheme use MD5 hash function which is huge computation overhead for resource constraint sensor nodes so proposed method use LOCHA: A Light-Weight One-way Cryptographic Hash Algorithm which is designed especially for resource-constrained sensors which leads to the supremacy of proposed method over the LoWaNa scheme. Future extension of the proposed method may be used for both message authentication and node authentication leading to the development of general-purpose security solution to Perception layer of IoT.

REFERENCES

1. Chowdhury, A. R., Chatterjee, T., & DasBit, S. “LOCHA: A light-weight one-way cryptographic hash algorithm for wireless sensor network” in 5th International conference on ambient systems, networks and technologies (ANT), procedia computer science, Vol. 32, 2014, pp. 497–504.
2. S. Kumar and D. R. Patel, “A survey on internet of things: security and privacy issues,” International Journal of Computer Applications, vol. 90, no. 11, 2014, pp. 20–26.
3. B. Przydatek, D. Song, and A. Perrig, “SIA: secure information aggregation in sensor networks,” in Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys ’03), ACM, November 2003, pp. 255–265.
4. R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark,” in Proceedings of the IEEE International Conference Image Processing (ICIP ’94), vol. 2, Austin, Tex, USA, November 1994, pp. 86–90.
5. C. Fei, D. Kundur, and R. H. Kwong, “Analysis and design of secure watermark-based authentication systems,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 1, 2006, pp.43–55.
6. I.Cox, M.Miller, J. Bloom, and J. Fridrich, “Digital Watermarking and Steganography”, Morgan Kaufmann, 2007.
7. W. Li and H. Song, “ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, 2016, pp.960–969.
8. S. Zhu, S. Setia, S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks”, in Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, 2003, pp. 62–72.
9. Perrig, Adrian, et al. “SPINS: Security protocols for sensor networks”, Wireless networks 8.5, 2002, pp. 521-534.
10. Kapoor, Vivek, Vivek Sonny Abraham, and Ramesh Singh. “Elliptic Curve Cryptography”, in ACM Ubiquity9.20, May 20-26, 2008.
11. Alrashed, Ebrahim A., Faruq Bagci, and Eman Alquraishi. “A key management approach for forward and backward secrecy in unattended WSNs”, in Journal of Engineering Research 4.4, 2017.
12. Conti, Mauro, et al. “Requirements and open issues in distributed detection of node identity replicas in WSN”, in IEEE International Conference on Systems, Man and Cybernetics. Vol. 2. IEEE, 2006.
13. Lv, Shaohe, et al. “Detecting the sybil attack cooperatively in wireless sensor networks”, in International Conference on Computational Intelligence and Security. Vol. 1. IEEE, 2008.
14. Zhang, Junqi, et al. “A dynamic authentication scheme for hierarchical wireless sensor networks”, in International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services. Springer, Berlin, Heidelberg, 2010.
15. Sen, Arpan, Tanusree Chatterjee, and Sipra DasBit. “LoWaNA: low overhead watermark based node authentication in WSN”, in Wireless networks 22.7 2016, pp. 2453-2467.
16. Cui, J.; Shao, L.; Zhong, H.; Xu, Y.; Liu, L. “Data Aggregation with End-to-End Confidentiality and Integrity for Large-Scale Wireless Sensor Networks” in Peer-to-Peer Netw. Appl. 2018, pp.11, 1022–1037. [CrossRef]
17. Yussoff, Y. M., Hashim, H., & Baba, M. D. “Identity based trusted authentication in wireless sensor network” in International Journal of Computer Science Issues (IJCSI) 2012, 9(3), pp.230–239.
18. Dong, X., & Li, X. “An authentication method for self nodes based on watermarking in wireless sensor networks” in International conference on wireless communication (WiCOM) 2009, pp. 4529–4532.
19. Kugler, P., Nordhus, P., & Eskofier, B.Shimmer “ Cooja and Contiki: A new toolset for the simulation of on-node signal processing algorithms” in International conference on body sensor networks 2013, pp. 1–6.
20. Sehgal, Anuj. "Using the contiki cooja simulator" Computer Science, Jacobs University Bremen Campus Ring 1 2013, pp. 28759.
21. Dunkels, A., Osterlind, F., & He, Z. "An adaptive communication architecture for wireless sensor networks” in International conference on embedded networked sensor systems (SenSys) 2007, ACM digital library, pp. 335–349.
22. Zhang, Guoyin, et al. “A new digital watermarking method for data integrity protection in the perception layer of IoT” in Security and Communication Networks 2017 .
23. Sun, Xingming, et al. “Digital watermarking method for data integrity protection in wireless sensor networks” in International Journal of Security and Its Applications 7.4, 2013 pp. 407-416.
24. Lalem, Farid, et al. “Data Authenticity and Integrity in Wireless Sensor Networks Based on a Watermarking Approach” in The Twenty-Ninth International Flairs Conference. 2016.
25. Shi, Xi, and Di Xiao. “A reversible watermarking authentication scheme for wireless sensor networks.” in Information Sciences 240, 2013, pp. 173-183.
26. Alromih, Arwa, Mznah Al-Rodhaan, and Yuan Tian. “A Randomized Watermarking Technique for Detecting Malicious Data Injection Attacks in Heterogeneous Wireless Sensor Networks for Internet of Things Applications” in Sensors 18.12, 2018 pp. 4346.
27. Kuhn, F., Wattenhofer, R., & Zollinger, A. “Ad hoc networks beyond unit disk graphs” in Proceedings of the 2003 joint workshop on foundations of mobile computing (DIALMPOMC’03),2003, pp. 69–78.

AUTHORS PROFILE

Neeraj Kumar is Assistant Professor in Shri Ramswaroop Memorial University Lucknow. He did his MTech (Computer Science and Engineering) from MANIT Bhopal, BTech (Computer Science and Engineering. He is having 7 years academic experience in the specializations of Operating Systems, Theory of Computation, Network Security, Internet of Things and Digital Forensics. He is active participant in various workshops and conferences conducted by IIT Bombay. He is working on research related to development of Lightweight Authentication mechanisms for resource scarce hardware such as Physical Things (Sensors and Actuators) in Perception Layer of Internet of Things. His current area of research is security of Internet of Things.

Dr. Deepak Singh Tomar is Associate Professor in MANIT, Bhopal. He did Ph.D. (Computer Science and Eng.), MTech, B.E. Computer Technology. He has 23 years’ experience in the specializations of Data Mining, Internet Technology, Network Security, Cyber Security & Cyber Forensics. He published total 59 Papers. He is active member of IEEE, International Association of Computer Science and Information Technology (IACSIT), Computer Science Teachers Association (CSTA), International Association of Engineers (IAENG) and International Webmasters Association (IWA). He guided 41 MTech and 5 PhD Thesis. His present area of research is Internet of Things security, Digital Forensics and secure architecture development for Web of Things.