International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1313-1320 www.ijaem.net ISSN: 2395-5252

An Enhanced Security System for Malicious Node Identification in Wireless Sensor Networks

[1]s.Swetha,

Pg scholar, master of engineering in applied electronics er. Perumal manimekalai college of engineering,hosur – 635117

Submitted: 25-06-2021 Revised: 06-07-2021 Accepted: 09-07-2021

ABSTRACT: Authentication serves as a critical property of secure communication to verify the identity of the entity involved in the communication. With the rapid development of wireless technologies, the flexible and cost-effective authentication is becoming an increasingly urgent demand for future wireless networks. This is because on one hand, the open and broadcast natures of wireless communications make wireless networks more vulnerable to spoofing attacks, where an unauthorized transmitter may impersonate as a legitimate one. On the other hand, with the wide deployment of Internet of things (IoT) and continuous evolvement of wireless technologies toward the fifth generation (5G) and beyond networks, it is foreseeable that future wireless networks will be consisted of a large number of heterogeneous devices, making cryptographic authentication techniques in wireless networks a challenging issue. Recently, physical layer authentication techniques, which exploit intrinsic and unique features of physical layer for authentication, have drawn a considerable attention to enhance and complement conventional cryptography-based authentication solutions. We focus on the study of physical layer authentication in a dual-hop wireless network with an untrusted relay and propose an end-to- end (E2E) channel based authentication scheme. This scheme fully utilizes wireless channel feature (i.e., channel impulse response in the dimensions of amplitude and path delay), and adopts artificial jamming technique, so that it is not only resistant to impersonate attack from an unauthorized transmitter but also resilient to replay attack from the untrusted relay. Finally, numerical and simulation results are provided by network simulator tool to illustrate both the efficiency of these theoretical results and evaluating the proposed technique prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

Keywords: Authentication, IOT, Wireless sensor networks,5G,Provenance,Cryptography,Spoofing attacks,Dual-Hop Wireless network.

I. INTRODUCTION

A computer network is a system in which computers are connected to share information and resources. The connection can be done as peer-to-peer or client/server. A computer network can also consist of, and is usually made for, more than two computers.

- You can play a CD music from one computer while sitting on another computer
- You may have a computer with a CD writer or a backup system but the other computer doesn't have it; In this case, you can burn CDs or make backups on a computer that has one of these but using data from a computer that doesn't have a CD writer or a backup system.

This project is to provide secure network provenance in the wireless sensor network.Wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations.A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable.

Every sensor node is equipped with a transducer,microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena.

The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery.It has the ability to correctly explain the system states is faulty or under attack. Provenance refers to the sources of information, such as entities and processes, involved in producing or delivering an artifact.The Provenance of information is crucial to making determinations about whether information is trusted, how to integrate diverse information sources, and how to give credit to originators when reusing information. Some part of the system is found to be in an unexpected state: for example, a suspicious routing table entry is discovered, or a proxy cache is found to contain an unusually large number of advertisements. The operators must determine the causes of this state before they can decide on an appropriate response. On the one hand, there may be an innocent explanation: the routing table entry could be the result of a misconfiguration, and the cache entries could have appeared due to a workload change. The goal is to extending and generalizing the concept of network provenance by adding capabilities needed in a forensic setting and developing techniques for securely storing provenance without trusted components by designing methods for efficiently querying secure provenance. Lightweight secure scheme-transmits each packet in WSN and IBF transmits the packet without any loss in a sensor network.

II.OBJECTIVE OF THE STUDY

This thesis exploits intrinsic and unique features of physical layer to authenticate transmitters for wireless communications. Our objective is to design flexible and cost effective authentication schemes to ensure the security of wireless communications. Towards this end, we first focus on authenticating transmitters in massive MIMO systems with non-ideal hardware, designing a new channel-based authentication.

Developing a new authentication scheme, which jointly utilizes two physical layer features (such as wireless channel and hardware features). Finally, we examine the E2E physical layer authentication in a dual-hop wireless network with an untrusted relay and propose an E2E channel based scheme which utilizes wireless channel feature (i.e., channel impulse response in the dimensions of gain and path delay).

Three commonly-used authentication performance metrics are of particular interest, which are false alarm (FA), missed detection (MD), and successful detection (SD) probabilities.

Here, FA occurs when a frame transmitted by legitimate transmitter is mistakenly regarded as unauthentic. When a frame originated from illegitimate transmitter is wrongly judged as authentic and SD occurs when a frame originated from illegitimate transmitter is successfully judged as authentic.

III. LITERATURE REVIEW

3.1 HARDWARE IMPAIRMENT-BASED AUTHENTICATION:

K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," IEEE Wireless Commun., vol. 17, no. 5, pp. 56–62, Oct. 2018.

- Hardware impairments-based authentication identifies transmitters by using inherent transmitter-specific hardware imperfections (e.g., phase noise and frequency error, in-phase/quadrature (I/Q), and carrier frequency offset (CFO)).
- Merits and demerits of these authentication solutions and the practical implementation issues are also discussed.

3.2Wireless Channel-Based Authentication:

L. Xiao, G. L. J, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," IEEE Trans. Wireless Commun., vol. 7, no. 7, pp. 2571–2579, Jul. 2019.

- The main idea of channel-based authentication is that channel state information is location-specific according to the radio propagation theory.
- It is difficult for an adversary to precisely build the same channel that is being used by a legitimate transmitter-received pair.

3.3 TAG-BASED AUTHENTICATION :

N. Xie and S. Zhang, "Blind authentication at the physical layer under timevarying fading channels," IEEE J. Sel. Areas Commun., vol. 36, no. 7, pp. 1465– 1479, Jul. 2018.

- The tag-based PHY-layer authentication, which embeds tag signals to modulated signals for identifying devices, is regarded as a promising authentication solution.
- This method has two major advantages over conventional authentication technologies.
- First, it enables a legitimate receiver to quickly identify transmitters without having to complete higher-layer processing.
- Second, embedding authentication tag into message signals and simultaneously transmitting them through wireless channels.

IV. PHYSICAL LAYER AUTHENTICATION

Authentication is a key security service verifying the claimed identity of a legitimate transmitter and rejecting an adversarial impersonation to secure communications. Therefore, providing flexible and cost-effective non-cryptography authentication paradigms is becoming more and more important and challenging for emerging networks (e.g., 5G and

IoT networks). This is mainly due to the following two reasons. The first one is that the broadcast nature of wireless medium makes communication systems more vulnerable to various attacks such as impersonation and replay attacks.

The other one is that mobile devices randomly join in or leave the network at any time, resulting in a challenging issue on the distribution and management of secret keys for cryptographic methods for emerging networks. Conventionally, authentication is implemented based on the cryptographic technique, where it is usually assumed that a secret key is shared in advance between the transmitter and receiver.

Nevertheless, the authentication relying on this assumption is increasingly being questioned in emerging network scenarios such as IoT, low power wide area networks and 5G wireless systems. This is mainly due to the reasons that distribution and management of secret keys become troublesome and even impossible.

The distributed nature of these scenarios makes the stored secret keys vulnerable to physical attacks. E.g., An attacker may capture a legal device and break the keys via hardware level attacks. Recent works in authentication exploit intrinsic and unique features of physical layer.

This draws considerable attentions to both research and academic communities on the development of novel physical layer authentication schemes to complement conventional cryptography-based solution such as authentication approach allows a receiver to quickly differentiate between legitimate and illegitimate transmitters, without having to complete higher-layer processing. Therefore, physical layer authentication is considered as a promising authentication solution for wireless communications, in which terminal devices might not be able to decode each other's higher-layer signalling, because they have different powers and computational capabilities at different levels of the hierarchical architecture.

Lots of research efforts have been devoted to the design of effective physical layer authentication schemes, such as channel-based authentication and hardware impairments-based authentication. The fundamental principle of channel-based authentication is that wireless channels are spatially de-correlated between different geographic locations, i.e., characteristics of channels between different transmitter & receiver pairs are significantly different. Hardware impairments-based authentication identifies transmitters by using inherent transmitter-specific hardware imperfections. (e.g., phase noise, frequency error).

4.1 Physical Layer Authentication for Massive MIMO Systems with Hardware Impairments

It is demonstrated that the presence of hardware impairments not only limits capacity but also deteriorates channel estimation accuracy in the high-power regime. Therefore, channel estimation accuracy is affected by hardware impairments, thermal noise, and multiuser interference. It is worth noting that for overall system.

Performance considering aggregate effect of all impairments has more substantial benefits than considering separately individual behaviour of each hardware module. Recently, increased attention has been focused on a novel system model with aggregate residual hardware impairments which are characterized by independent additive distortion noises at base station and user terminals.

Hardware impairments need to be deliberately considered in the design of future effective physical layer authentication schemes.

In massive multiple-input multiple-output (MIMO) systems, which will serve as an essential technology in meeting the continuously increasing throughput demands and spectrum efficiency for the fifth generation (5G) and beyond networks. Based on this background, this work studies transmitter authentication in massive multiple-input multiple-output (MIMO) systems with non-ideal hardware for 5G and beyond networks. The main contributions of this work are summarized as follows:

- By utilizing location-specific property of wireless channels and considering hardware impairments to authenticsssssssate transmitters, we first develop a new channel-based authentication scheme for massive MIMO systems with non-ideal hardware.
- To calculate the quantity caused by hardware impairments on authentication performance, we formulate channel estimation under hardware impairments and determine error covariance matrix based on linear minimum mean square error technique.
- Using the quantization result, matrix and hypothesis testing theories, we analytically model FA and SD probabilities under different channel covariance matrix models. Simulation results are also provided to validate theoretical modelling of the two probabilities.
- Through the theoretical models, we further examine how different levels of hard ware impairments impact authentication performance, and also determine how to set antennas correlation pattern and the number of base station antennas to achieve a required authentication performance.

4.2 Physical Layer Authentication Jointly Utilizing Channel and Phase Noise in MIMO Systems

Extensive research efforts have been devoted to the study on joint estimation of channel and phase noise in MIMO systems. The problem of joint estimation of channel and phase noise is considered using data-aided and decision-directed weighted least-squares approaches in MIMO systems.

These works mainly focus on joint estimation of channel and phase noise without taking important security issue into account in MIMO systems.

To the best of the author's knowledge, how to develop a flexible and cost-effective authentication scheme by jointly utilizing the wireless channel and hardware features has not been considered. Based on the above background, we explore physical layer authentication by jointly taking wireless channel and hardware features into account for authentication in heterogeneous coexist MIMO systems. The main contributions of this work are summarized as follows:

- By utilizing two physical layer features in terms of location-specific channel gains and transmitter-specific phase noise to authenticate transmitters, we propose a simple and flexible physical layer authentication scheme in MIMO systems to differentiate between legitimate and illegitimate transmitters. We analyse three properties of this scheme: Covertness, Robustness and Security which are three important aspects to assess authentication schemes.
- To formulate variances of estimation errors in terms of channel gains and phase noise, we adopt a maximum-likelihood estimator (MLE) to estimate channel gains and soft-input extended Kalman filter (EKF) to track phase noise over a frame, and then quantize the temporal variations of channel gains and phase noise through the developed quantizers.
- By using quantization results and theories of hypothesis testing and stochastic process, we derive the closed-form expressions for FA and MD probabilities with a careful consideration of quantization errors. Simulation results are also provided to validate theoretical models for the two probabilities.
- Through theoretical models, we further investigate how thresholds (for channel gain, phase noise, and decision) can impact the authentication performance. Guidelines for properly setting these parameters are also provided to achieve a desired authentication performance.

4.3 End-to-End Physical Layer Authentication for Dual-Hop Wireless Networks

- Existing works mainly focus on one-hop physical layer authentication, where transmitters and receivers can communicate with each other directly.
- In the large-scale distributed wireless networks such as IoT and 5G wireless systems, E2E communication is usually conducted with the help of relay(s). Due to transmission efficiency, delay and secrecy constraints the multi-hop E2E physical layer authentication is an important research issue in wireless communication scenarios, where relay only needs to amplify and forward the signals transmitted by the transmitter to the legitimate receiver or to decode the signals and then forward them to the legitimate receiver.
- To the best of our knowledge, the multi-hop E2E physical layer authentication is still not well-explored.Notice that the available one-hop physical layer authentication schemes cannot be directly extended to multi-hop E2E physical layer authentication mainly due to the following challenges.
- First, the cascade channels between the transmitter and receiver become much more dynamic and complicated, making multi-hop E2E physical layer authentication more challenging.
- Second, the relay can be potential adversary to record the received signals and initiate replay attacks, bringing new threat to the E2E physical layer authentication. As one step towards the study of E2E multi-hop physical layer authentication, this work focuses on the channel-based E2E physical layer authentication in a dual hop wireless network with an untrusted relay. This is because the dual-hop wireless networks are simple and serve as a foundation for the study of general multi-hop wireless networks.
- By carefully exploiting the highly dynamic properties of the dual-hop cascade channels, we develop an efficient E2E physical layer authentication scheme to discriminate transmitters at different locations. The main contributions of this work are summarized as follows.

We propose a new E2E physical layer authentication scheme for dual-hop wireless networks with an untrusted relay. This scheme utilizes the location-specific features of both channel gain (CA) and delay interval (DI) of cascaded channels to discriminate transmitters, and adopts the artificial jamming technique to resist against possible replay attack from the untrusted relay.

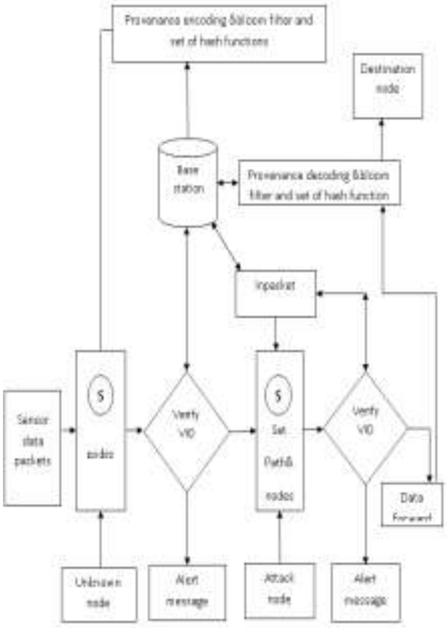
• Using statistical signal estimation theory and the two-dimensional quantizers, we can qualify the temporal variations of CA and DI of cascaded multipath channel.

• Based on the hypothesis test theory, theoretical analysis is then conducted to derive the expressions for FA and MD probabilities, such that E2E authentication performance under the proposed E2E physical layer authentication scheme can be fully depicted.

• Finally, extensive numerical/simulation results are provided to validate theoretical results for FA and MD probabilities and to illustrate performance for the proposed scheme.

Towards this end, we first focus on authenticating transmitters in massive MIMO systems with non-ideal hardware, designing a new channel-based authentication scheme with hardware impairments taken into account. We then develop a flexible and cost effective authentication scheme, which jointly utilizes two physical layer features (such as wireless channel and hardware features). Finally, we examine the E2E physical layer authentication in a dual-hop wireless network with an untrusted relay and propose a corresponding physical layer authentication scheme which utilizes wireless channel feature (i.e., channel impulse response in the dimensions of gain and path delay).

V. PROPOSED BLOCK DIAGRAM



Proposed a distributed mechanism to encode provenance at the nodes and a centralized algorithm to decode it at the BS by using vertex id and analyzed with **NS2 simulator**.

The technical core of our proposal is the notion of in packet Bloom filter. Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance in the **same channel**. Emphasize that our focus is on securely transmitting provenance to the BS.

VI.SYSTEM REQUIREMENTS

Hardware requirement

- **Processor : Pentium dual core**
- **Ram : 1GB.**
- **Hard Disk : 80 GB.**
- **Compact Disk : 650 Mb.**
- **Input device :Mouse → Logitech.**

:Keyboard→ 110 keys

- **Output device : VGA and High Resolution**
- **Monitor :17” Colour Monitor.**

Software requirement

- **Front End/GUI Tool : Cygwin/NS2**
- **Operating System : Windows 7**
- **Script : TCL**

VII.EXPLANATION OF ALGORITHM AND THEIR PROCESS

7.1 PROVENANCE ENCODING

The provenance record of a node includes
1) the node ID and
2) an acknowledgement of the observed packet in the flow.

The acknowledgement can be generated in various ways to serve this purpose a node must maintain a per-flow record to store the previous packet sequence for each data flow that passed through the node.

If a node receives a packet from a data flow for which it has no previous packet information, then it may use a pre-specified special purpose identifier, such as 0, as the previous packet sequence.

This addresses the case of routing path changes where a new node in the path can use this special identifier for encoding provenance.

7.2 PROVENANCE DECODING

The BS stores and updates the latest packet sequence number for each data flow. Upon receiving a packet, the BS recovers the preceding packet sequence transmitted by the source node from the packet header, fetches the last packet sequence for the flow from its local storage and utilizes these two sequences in the process of provenance verification and collection.

7.3 PROVENANCE VERIFICATION

The BS conducts the verification process not only to verify its knowledge of provenance but also to check the integrity of the transmitted provenance. Assume that the knowledge of the BS about this packet's path is P0. At first, the BS initializes a Bloom filter BFc with all 0's. The BF is then updated by generating the VID for each node in the path P0 and inserting this ID into the BF. BFc now reflects the perception of BS about the encoded provenance. To validate its perception, the BS then compares BFc to the received IBF .

The provenance verification succeeds only if BFc is equal to IBF. Otherwise, if BFc differs from the received IBF, it indicates either a change in the data flow path or a BF modification attack.

The verification failure triggers the provenance collection process which attempts to retrieve the nodes from the encoded provenance and also to distinguish between the events of a path change and an attack.

7.4 PROVENANCE COLLECTION

The provenance collection scheme makes a list of potential vertices in the provenance graph through the ibf membership testing over all the nodes. For each node in the network, the BS creates the corresponding vertex (i.e., vi with VID vidi).

The BS then performs the membership query of vidi within i.e., the host node ni is in the data path. Such an inference might introduce errors because of false positives (a node not on the route is inferred to be on the route).

- A distributed mechanism to encode provenance at the nodes and a centralized algorithm to decode it at the BS by using vertex id and analyzed with **NS2 simulator**.
- The technical core of our proposal is the notion of in packet Bloom filter. Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance in the **same channel**. Emphasize that our focus is on securely transmitting provenance to the BS.

VIII.NETWORK SIMULATOR - NS-2

NS-2 is an open-source simulation tool running on Unix-like operating systems. It is a discrete event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks.

It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic.

8.1 NS-2 IMPLEMENTING LANGUAGES

NS-2 is basically written in C++, with a TCL (Object Tool Command Language) interpreter as a front-end. It supports a class hierarchy in C++, called compiled hierarchy and a similar one within the TCL interpreter, called interpreter hierarchy. Some objects are completely implemented in C++, some others in TCL and some are implemented in Rainer Baumann, ETH Zurich 2004 Master's Thesis Vehicular Ad hoc Networks (VANET) baumann@hypert.net 28/128 both. For them, there is a one-to-one correspondence between classes of the two hierarchies.

But why should one use two languages? The simulator can be viewed as doing 2 different things. While on one hand detailed simulations of protocols are required, we also need to be able to vary the parameters or configurations and quickly explore the changing scenarios.

For the first case we need a system programming language like C++ that effectively handles bytes, packet headers and implements algorithms efficiently. But for the second case iteration time is more important than the run-time of the part of task. A scripting language like TCL accomplishes this.Ns2 is an open source model,in which it is easily available.

The code for this, can be easily modified for different applications. The versions of ns2 is ns2.32, ns2.33, ns2.34, ns2.35. The (NAM) Network animator is a graphical view of network simulator.Ns2 is a packet level simulator. The complex system can be easily tested and simulated. Front end is OTcl and back end is C++ event simulator.

ADVANTAGES OF NS2

- ➢ NS-2 is the most widely used simulator for ad hoc wireless simulations. It is an open source, freely downloadable piece of software, which runs on Linux Platform.
- ➢ NS-2 is easily extensible; any extension to existing ad hoc routing protocol can be implemented with ease.

Since most of the currently published results for MANETs have used NS-2 for simulation too, for fair comparison.

Algorithm-1 Provenance Verification:

- **Input: Received packet with sequence seq and iBF ibf.**

Step 1:Set of hash functions H, Data path P = < n l 1 , ..., n 1 , ..., n p >

Step 2:BF c ← 0 // Initialize Bloom Filter for each

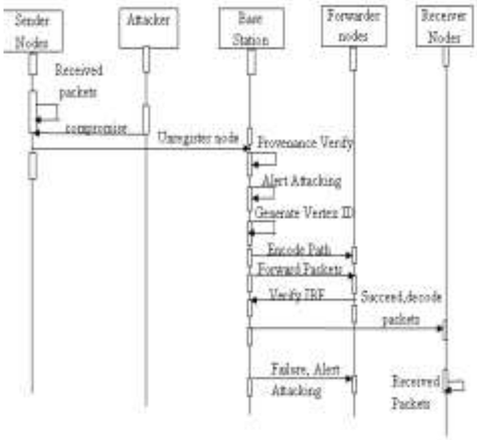
```
n i ∈ P do
vid i = generateVID (n i , seq)
 Step 3:Insert vid i into BF c using hash functions in H endfor
if (BF c = ibf ) then
return true // Provenance is verified endif
return false
```

Algorithm-2 Provenance Collection:

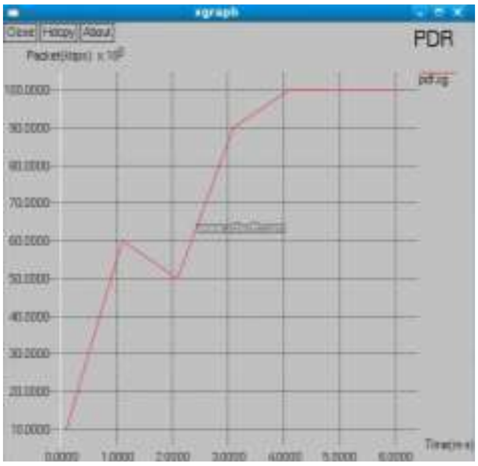
- **Input: Received packet with sequence seq and iBF ibf. N Set of nodes (N) in the network, Set of hash functions H**

```
Step 1: Initialize
Set of Possible Nodes S ← ∅
Bloom Filter BF c ← 0 // To represent S
Step 2:Determining possible nodes in the path and build the representative BF
for each node n i ∈ N do
vid i = generateVID (n i , seq)
if (vid i is in ibf ) then S ← S ∪ n I
Step 3:Insert vid i into BF c using hash functions in H
endif endforVerify BF c with the received iBF if (BF c = ibf ) then
return S // Provenance has been determined correctly else
return NULL // Indicates an in-transit attack
endif
```

IX. SEQUENCE DIAGRAM



X.PACKET DROP RATE



XI.ADVANTAGES AND DISADVANTAGES

ADVANTAGES

- Proposed scheme is effective,light weight,scalable and high throughput.
- The traditional cryptographic approaches, physical layer security (PLS) takes advantage of the intrinsic characteristics of wireless channels, such as noise, fading, and interference, to boost the signal reception at the legitimate receiver and degrade the received signal quality at the eavesdropper.
- Provisioning techniques, physical layer security (PLS), this can provide unbreakable secure transmission problems with limited feedback.

DISADVANTAGES

- As opposed to existing research separate transmission channels for data and provenance, only require a single channel for both. Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures, and they employ append-based data structures to store provenance, leading to prohibitive costs.

XII.CONCLUSION AND FUTURE SCOPE

Addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance, extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental results analysed with ns2 simulator show that the proposed scheme is effective, light-weight, scalable and high throughput.

- The goal is to extending and generalizing the concept of network provenance by adding capabilities needed in a forensic setting and developing techniques for securely storing provenance without trusted components by designing methods for efficiently querying secure provenance.
- An improved accuracy of packet loss detection is done in the case of multiple consecutive malicious sensor nodes.
- In future work, we plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection.

REFERENCES

[1]. Andrews J.G, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, “What will 5G be?” IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[2]. Chai-et-al,Qing-Wei Chai,Wei-Min Zheng,”A Parallel WOA with two communication strategies applied in DV-Hop Localization method”,EURASIP journal on wireless communication and networking 2020.

[3]. Christof P, J. Pelzl, and B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010.

[4]. Deng X and Yang Y “Online adaptive compression in delay sensitive wireless sensor networks,” IEEE Trans. Comput., vol. 61, no. 10, pp. 1429–1442, Oct. 2012.

[5]. Diffie W and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[6]. Imran et al,Md Abdullah AI Imran,”Optimal operation mode selection for energy-efficient light weight multi-hop time synchronization in linear wireless sensor networks”,EURASIP journal on WCN 2020.

[7]. Kartalopoulos S.V, “A primer on cryptography in communications,” IEEE Commun. Mag., vol. 44, no. 4, pp. 146–151, Apr. 2006.

[8]. Lin J, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125– 1142, Oct. 2017.

[9]. Polak and D. L. Goeckel, “Identification of wireless devices of users who actively fake their rf fingerprints with artificial data distortion,” IEEE Tran. Wireless Commun., vol. 14, no. 11, pp. 5889–5899, Nov. 2015.

[10]. U. Raza, P. Kulkarni, and M. Sooriyabandara, “Low power wide area networks: An overview,” IEEE Commun. Surveys and Tutorials, vol. 19, no. 2, pp. 855–873, Jan. 2017.

[11]. Shen, T. Zhang, Y. Wang, H. Wang, and X. Jiang, “Microthings: A generic IoT architecture for flexible data aggregation and scalable service cooperation,” IEEE Commun. Mag., vol. 55, no. 9, pp. 86–93, Sep. 2017.

[12]. Wang et al-journal,”The energy efficient MDA-SMAC protocol for the wireless sensor networks” Journal paper 2020.