International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

An Efficient Location Based Key Management Approach for WSN

P. Ganapathiammal[1], Dr J.B. Shajilin Loret[2]
[1]Department of IT, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India
[2]Assistant Professor, Department of IT, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

ABSTRACT

With the advent of 5G, technologies such as Software-Defined Networks (SDNs) and Network Function Virtualization (NFV) have been developed to facilitate simple programmable control of Wireless Sensor Networks (WSNs). However, WSNs are typically deployed in potentially untrusted environments. Therefore, it is imperative to address the security challenges before they can be implemented. In this paper, we propose a software-defined security framework that combines intrusion prevention in conjunction with a collaborative anomaly detection system. Initially, an IPS-based authentication process is designed to provide a lightweight intrusion prevention scheme in the data plane. Subsequently, a collaborative anomaly detection system is leveraged with the aim of supplying a cost-effective intrusion detection solution near the data plane. Moreover, to correlate the true positive alerts raised by the sensor nodes in the network edge, a Smart Monitoring System (SMS) is exploited in the control plane. The performance of the proposed model is evaluated under different security scenarios as well as compared with other methods, where the model's high security and reduction of false alarms are demonstrated.

I. INTRODUCTION

A vision is emerging of the convergence of wireless communications, embedded sensing and processing devices with distributed algorithms into the field of wireless sensor networks (WSNs). The proponents of this emerging technology envision a future in which environments from nature reserves to cities are instrumented with disposable computing nodes, each with an on board radio transceiver, battery, environmental sensors and processing capabilities. Wireless sensor network research grew out of the distributed sensor networks project at the Defence Advanced Projects Research Agency (DARPA) [5], although the technology of the 1970s limited processing and communications and restricted the nodes to large form factors. With the exponential progress and cost reduction in micro processing during the 1990s and 2000s, many new applications for WSN deployment emerged. The Amorphous Computing project [6] envisioned highly generic, cheap and indistinguishable miniature devices, operating by analogy to the individual cells of biological systems. Since then, deployment of wireless sensor networks has been considered for diverse spectrum domains, including logistics [7], medicine [8], environmental monitoring [9] [10], military monitoring [11] and surveillance [12].

II. APPLICATIONS OF WSN

The outstanding progress in natural philosophy, technology sealed the trail for the expansion of micro-electronics, thus facilitating the manufacture of tiny chips and small devices. The communication technology is undergoing transformation because of the planning and improvement of small devices and thus expedited the planning and advancement of WSN with low price and low energy consumption.

WSN has many applications in military, health and in different industrial sectors. Due to the characteristics of WSN, sensor nodes are typically attributed with restricted power, low information measure, low memory size and restricted energy. Due to the measurability and energy effectiveness options, investigators prompt many routing protocols for cluster-based WSN. Routing could be a method of determinative a path between supply and destination upon request of information transmission. In WSN, the network layer is employed to implement the routing of the incoming information.

It is illustrious that in multi-hop networks the sensing node cannot reach the sink directly. So, intermediate detector nodes have to be compelled to relay their packets. The implementation of routing tables offers the answer. These contain the lists of node possibility for any given packet's destination.

Numerous improved hierarchal routing protocols were suggested in many research papers. But, some requirements for the routing protocols are conflicting. Always selecting the shortest route towards the base station causes the intermediate nodes to deplete faster, which result in a decreased network lifetime. At the same time, always choosing the shortest path might result in lower energy consumption and lower network delay. Since the routing objectives are tailored by the application, different routing mechanisms have been proposed for different applications. These routing mechanisms primarily differ in terms of routing objectives and routing techniques.

The majority routing protocols are vulnerable to uncounted security risks. Attacks comprising Cluster Head 2(CH) are in the main harmful. Because of resource restrictions, the general public key based algorithms like Rivest Shamir Adelman (RSA) and Diffie-Hellman are terribly complicated and energy-consuming for WSN. In several cases, multiple sensing element nodes are needed to beat environmental obstacles like obstructions and line of sight constraints. Also, the setting to be monitored doesn't have an associate degree of existing infrastructure for energy economical communication. Therefore, it becomes imperative for sensing element nodes to survive on tiny, finite sources of energy and communicate through a wireless communication. Security could be a crucial issue because of inherent limitations in WSN.

III. WSN MODEL

Unlike their ancestor ad hoc networks, WSN are resource limited, they are deployed densely, they are prone to failures, the number of nodes are several orders higher than that of ad hoc networks, their network topology is constantly changing, they use broadcast communication mediums and finally wireless sensor nodes does not have global identification tags.

SENSOR FIELD:

A sensor field can be considered as the area in which the nodes are placed.

SENSOR NODES:

Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to the sink.

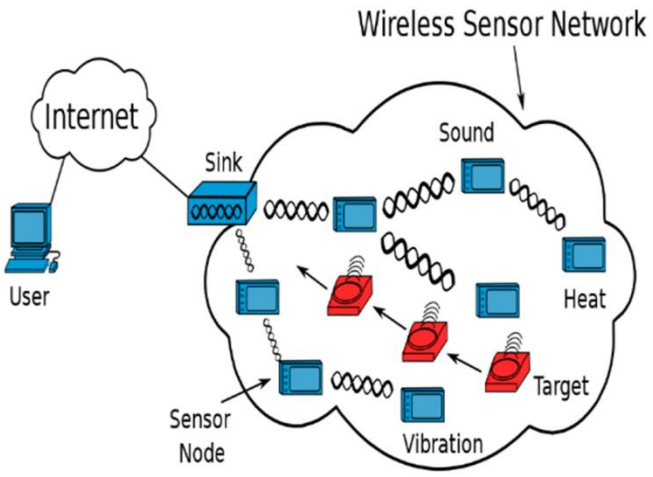


Figure 1.1 Components of WSN

SINK:

A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network.

TASK MANAGER:

The task manager is the centralized point of control within the network, which extracts information from the network and disseminates control information back to the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and also an access point for a human interface. This can be either a laptop or a workstation.

IV. WSN IMPLEMENTATION FRAME WORK

The literature and information on WSN applications, solutions, scientific and technological development are abundant. Internet and Mica (The platform is named Mica due to its resemblance with the finalelectronic implementation of silicate relative) mote based WSN implementation were briefed here.

4.1 PRESENT METHODOLOGIES

Internet based WSN is a good substrate for WSN implementation. The altered TCP for WSN is good with a few arrangements accessible at the physical, data link, network, transport, and application layers of the OSI model, which rearranges WSN configuration and operation. The topologies and administration of the system are adaptable. Applications with diverse prerequisites can be obliged. Mica motes are commonly planned in stackable layers. The center of a mote is a little, minimal effort, low-control PC. The PC screens, one or more sensors and unites with the outside world with a radio connection. Most of the time, they remained in a standby mode for power saving purpose. Several times in each second, the device flicks on its radio to check for incoming messages, but if there are none, the radio is shut off within milliseconds. Similarly, the sensors usually take their readings only once every few minutes. Data is transmitted only when the memory is full. Motes Operating System (MOS) forces mote programs to shut down except when certain events that warrant action occur. The operating system is also highly modular. If a program needs only certain functions from MOS, the nonessential parts of the operating system are automatically removed from the mote.

4.2 FUTURE REQUIREMENTS

Applications requiring additional measurements and additional activity points are in demand. Necessary applications could need massive or extraordinarily massive mounted fixed or mobile networks, for which, WSN are the natural answer. However, many challenges at completely different levels have to be faced, specifically hardware, software, sensors and node sizes, power they will harvest or store, harsh environmental in operating conditions, node failures, quality of nodes, dynamic topology, communication failures, heterogeneousness of nodes, massive scale of

deployment, unattended operation, schedule, period of time maximization, robustness, fault tolerance, self-configuration, and security.

Power:

The current technologies already permit extended operation using small size, low Ampere-hour batteries. This is achieved with both low power consumption components as well as by keeping the nodes in stand-by as long as possible. However, some applications will surely require battery recharge. Sun, Wind vibration and Bio energy are some of the possible solutions already under study.

Network programming and re-programming:

Programming of a wireless network with many nodes is not easy. New solutions have to be found. To replace the software on motes with updated versions, an idea based on the way viruses and worms are spread on the Internet, have been tried.

The new program is packaged into a special form and delivered to the root mote, which installs it and infects its neighbors with the package. The upgrade makes its way through the network like an epidemic, but it does so in a more controlled fashion that avoids redundant communications and adapts to the way that the motes are scattered in space.

Node failure:

A WSN is unlikely to crash outright, but as some nodes die and others generate noisy or corrupted data, the measurements of the overall system may become biased or inconsistent. Work has been done on techniques to judge the health of a WSN by perturbing the system in a controlled way and observing how the sensor nodes respond.

Privacy:

Over the next decade or so, wireless sensor nodes will probably evolve into a much less distinct and less visible form. Devices will gradually migrate out of their little boxes and will instead be incorporated directly into various materials and objects. Many of them will draw energy directly from the environment in which they operate.

To the extent that these kinds of WSN infiltrate homes, workplaces, farms, transportation terminals and shopping sites and are able to sense the presence, motion and even physiological states of individuals, they will raise substantial privacy concerns. Privacy issues are quite straightforward for many valuable applications, but in other domains, a careful balance must be struck to ensure that the technology properly empowers the individual.

The present technologies limit a WSN in hardware related aspects like sensed quantities, the size of nodes, and nodes autonomy, but it is at the software level where improvements and new solutions are required. All these developments must produce very low-cost devices so that the cost of a WSN with a large number of nodes is not prohibitive.

V. ROUTING IN WSN

One of the fundamental configuration objectives of WSN is to do information correspondence while attempting to draw out the lifetime of the system and forestall integration debasement by utilizing forceful vitality administration methods. The configuration of steering conventions is affected by numerous testing elements as given underneath:

5.1 Node Deployment

Node organization in WSN is application-particular and can be either manual (deterministic) or randomized. In manual sending, the sensors are physically put and information is directed through

foreordained ways. On the other hand, in arbitrary arrangement, the nodes are scattered arbitrarily, making a specially appointed directing framework.

5.2 Energy Consumption

Sensor node lifetime depends enormously on battery lifetime. In the multi-bounce WSN, every node assumes a double part as information sender and information switch. The breaking down of some sensor nodes emerging out of force disappointment can bring about critical topological changes and may oblige re-directing of parcels and revamping of the system.

5.3 Fault Tolerance

Some sensor nodes may come up short or be obstructed because of absence of force, physical harm or natural impedance. The disappointment of sensor nodes ought not to influence the general functionalities of the sensor system. The steering convention needs to focus the other conceivable way to course the information to the sink node.

5.4 Scalability

The quantity of sensor nodes conveyed in the detecting zone may be in the request of hundreds or thousands, or considerably more. Any directing plan must be scaled up to handle steering, among the immense number of sensor nodes. By and large nodes in the sensor system are in rest mode and at whatever point an occasion is detected, the nodes are changed over to dynamic state.

5.5 Coverage

In WSN, every sensor nodes gets a certain perspective of the earth. A given sensor's perspective of the earth is constrained both in extent and exactness. It can just cover a constrained physical range of the earth. Subsequently, range scope is additionally a vital configuration parameter in WSN.

In a WSN, the network data between the nodes are traded when sending them. However the learning about node's area is needed in numerous sensor system applications. This area data empowers early expectation of the marvel, along these lines, minimizing the impact of unsafe fiasco. In directing, the area data of nodes aided in simple discovery of steering way between the source and the destination which thusly minimizes the inertness included in information transmission.

VI. CLASSIFICATION OF WSN ROUTING PROTOCOLS

Routing protocols are often classified as Proactive, Reactive and Hybrid looking on the sort of communication routes processed at intervals the network for information transmission from the supply to sink. In Proactive routing protocols all the routes are calculated before the sink makes associate initiation to speak with the nodes within the network, wherever as in Reactive routing protocols, the trail values square measure calculated only if needed. Whenever a sink needs to contact a specific node, the path values were calculated and therefore the best path is chosen for information transmission. Hybrid routing protocols, as the name suggests, is a combination of both proactive and reactive routing protocols, which decides when to calculate the path from the sink to the source depending on the type of communication. Generally, it has been suggested that proactive routing protocols are better for static nodes. The reason is that a lot of energy can be saved compared to reactive routing protocols which depend on the discovery of the best route path for data transmission. In proactive routing it is not necessary to search for the nearest neighbors for every next hop when data is transmitted. The routing protocols in WSN can be coarsely divided into the following two categories:

- Based on Network Structure, which can be sub divided as Flat, Hierarchical and Location Based protocols.
- Based on Protocol Operation, which can be sub divided as Negotiation based, Multi-Path based, Query based, QoS based and Coherent based routing protocols. Directing is one of the basic assignments in WSN. Restricted to conventional specially appointed systems, steering in WSN is additionally difficult as an after effect of its inalienable qualities. Firstly, assets are extraordinarily obliged as far as power supply, preparing ability and transmission data transfer capacity. Also, it is hard to plan a worldwide tending to plan like an Internet Protocol (IP). Besides, IP can't be connected to WSN, since location redesigning in an expansive scale or element WSN can bring about overwhelming overhead. Thirdly, because of the constrained assets, it is hard for a directing convention to adapt to eccentric and regular topology changes, particularly in a versatile domain. Fourthly, information accumulation by numerous sensor nodes more often than not brings about a high likelihood of information excess. Fifthly, most uses of WSN require the normal correspondence plan of numerous toone, i.e., from various sources to one specific sink, as opposed to multicast or shared.

VII. MOTIVATION

The long run goal of this analysis is to support high speed, energy economical knowledge delivery to the service-oriented specification in an urban setting that provides distinctive services to the user. There are several potentialities which might create the urban setting actually awake to the wants of the user. This level of responsiveness and interactivity between the user and, therefore, the urban setting take the client expertise to a replacement level. Some of the applications facilitated by such a network layer protocol could be advertisements and offers based on the proximity to a shop, display of user-selected content on public displays, asking a user to switch off the phone in a silent zone (e.g. conference hall), enabling a user to change the Air Conditioner (AC) temperature or switch it off in a certain area and providing security messages in case the user goes in a restricted area. These applications and much more can be implemented at the application layer with the help of this work.

VIII. EXISTING WORK

Wireless Sensor Networks (WSNs) provide infrastructure-free communications over the shared wireless channels without the need for fixed infrastructures or centralized access points. Sensor networks comprise of a set of dynamic cooperating nodes; forming one of the most promising wireless technologies which introduce a new wireless transmission paradigm by employing multihops for information transfer. WSNs have significant potential applications in the fields of transportation, agriculture, industrial automation, process monitoring, military surveillance, environment monitoring, health-care, etc. According to, these wireless sensors need to be self-configured into a network to process and interpret sensor measurements, and convey this information to a centralized control location.

Moreover, traditional WSNs typically consist of routers and switches as network devices. Therefore, as they grow, they become difficult to monitor and update. Meanwhile largescale WSNs are also heterogeneous due to the use of different communication protocols, which fundamentally means they consist of different network clusters that only cooperate at low level of communication [2]. Since the distributed management of a communication protocol determines which node can receive or transmit data, this makes the global vision and the applicability of security mechanisms in the network a very complex task. Further, as the scale of

the WSN expands, it is faced with several constraints, such as resource and energy restrictions, processing, memory, and communication capabilities. To address these constraints, the deployment of a lightweight security framework which includes the centralization of intelligent features becomes essential.

With the emergence of 5G, promising technologies such as Software-Defined Networks (SDNs) and Network Function Virtualization (NFV) have been designed to support innovations and enable simple programmable control of data paths in wireless sensor nodes [3]. These technologies provide WSNs with the capability of being programmed upon request. In addition, they allow multiple isolated sensor functions, by addressing and forwarding mechanisms, to share the same physical infrastructure. Furthermore, SDNs allow network administrators to manage network services through the abstraction of lower level functionalities. This is done by decoupling the control plane that makes decisions about where traffic is sent from the underlying data plane to the selected destinations. As a consequence, computational complexity is reduced while throughput is enhanced. In addition, the SDN approach to WSNs seeks to alleviate most of the challenges and ultimately foster efficiency and sustainability in WSNs.

Thus, the control plane can dynamically enforce flow rules when the data plane requires it. However, this control operation can cause serious problems when there are excessive requests from the data plane to the control plane. On the other hand, if the data plane receives many requests in a short period of time, it can flood the messages to the control plane. Moreover, a flow table in the constrained data plane can also be flooded by rules for handling requests.

Despite the high programmability and automation of WSNs gained from 5G, these networks are not immune to malicious users. Since, network intelligence is centralized in SDN controllers, protecting the communications throughout the data and the control planes is critical [5]. For instance, the centralized network intelligence might become victim of malware [6].

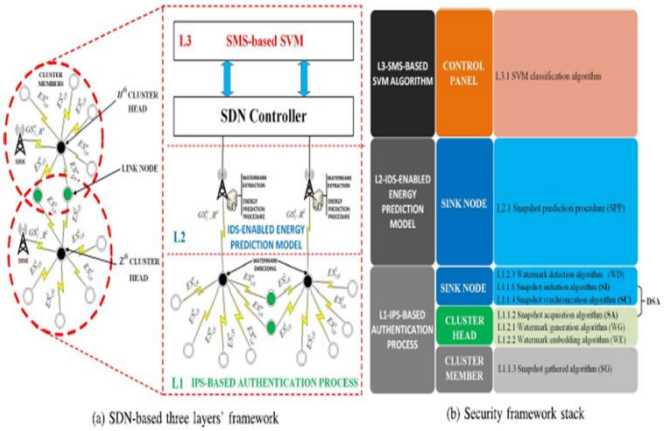
In the SDN environment, some WSN-unique data plane threats can take place. Under such scenarios, fake traffic flows caused by both flawed devices and malicious sensor nodes can compromise the entire SDN architecture. Similarly, OpenFlow switches and resource-constrained nodes can be disrupted by network elements infected with Denial of Service Attacks (DoS) such as Black hole attacks, Selective Forwarding attacks, Hello Flood attacks, and Sybil attacks [6], [7]. It is evident from the above discussion that the disruptive SDN technology is also prone to different attack vectors.

In this vein, several works have been proposed to leverage the benefits of the SDN architecture for enhanced network security such as virtual firewall, access control, and deep packet inspector systems [6]. Motivated by their findings, the major contribution of the proposed work is on addressing the security issues prevalent in the SDN's data plane. In this direction, the work emphasizes the problem of authentication and high-precision anomaly detection in the untrusted and resource-constrained data plane of SDNs.

IX. RELATED WORK

A plethora of research works have been performed to address high security and low-latency solutions for resource constrained WSNs. In this context, some of the existing IPSbased authentication procedures have been developed using classical key management authentication mechanisms. For example, an IPS combining Internet Protocol (IP) trace-back with an enhanced adaptive acknowledgment (EAACK) was proposed in [16]. Moreover, Location-Based Keys (LBKs), binding private keys of individual nodes to both their identifications and geographic locations was proposed in [17]. These approaches improved the security at the cost of increasing the latency of the network. To address the challenges associated with

the low-latency requirements, some works used physical



(a) SDN-based three layers' framework (b) Security framework stack

Fig. 3.1. A collaborative security framework for SDWSNs.

layer features. For instance, a two-factor user authentication mechanism was recommended in [18], where the authors devised an authentication mechanism comprising of registration and authentication phases. Furthermore, the authors in [19]–[21], explored a biometric-based continuous authentication technique, without the the need for an authentication server. These approaches reduced the latency but at the cost of increasing the complexity of the authentication procedures.

Furthermore, some works also exploited physical layer features in IDS to achieve low-latency in WSNs. In this context, a novel intrusion detection scheme based on energy prediction for cluster-based WSNs was introduced in [22], wherein the authors used the energy states of wireless sensor nodes to predict malicious behaviors at a given time. Excessive false alarms are a common artifact of these approaches. Consequently, machine learning procedures have been widely used to develop IDS-based solutions. For instance, the use of neural networks and watermarking techniques was suggested in [23]. A SVM methodology was proposed in [24], while a hybrid machine learning approach for network anomaly detection was put forward in [13]. A hybrid anomalybased IDS was recommended in [12] which employed SVM and multi-layer perceptron (MLP) to identify anomalies in the network. Further, the authors in [25] presented an intrusion detection engine based on neural networks combined with a protection method-based on a watermarking technique. While these algorithms improve the accuracy of network anomaly detection models, they also introduce high computational cost which is inadequate for WSNs. Even though relevant works have been proposed in the literature to target security issues in SDWSNs, challenges such as high security, excessive false alarms, low-latency, and high computational cost still remain unaddressed.

X. CONTRIBUTIONS

To address these imperative challenges, in this paper, a bottom-up security framework is designed. The novelty of the proposed work lies in devising and evaluating a collaborative framework which amalgamates a recurrent lightweight authentication method in conjunction with an intrusion detection and authentication method in conjunction with an intrusion detection and a real-time smart monitoring system; achieving lightweight authentication and enhanced anomaly detection mechanisms in SDWSNs. Since a single-gateway (cluster head) architecture is not scalable and might cause an incremental overhead in largescale WSNs, the proposed work uses a cluster-based SDWSN architecture that provides a hierarchical organization to a flat sensor network topology, considerably reduces the latency of the network [26]. This architecture consists of four kinds of dynamic nodes, namely, cluster members, cluster heads, link nodes, and sink nodes. Further, in this framework, a Distributed

Snapshot Algorithm (DSA) is executed to capture network snapshots periodically so as to obtain the global energy state of the WSN; wherein the global energy state corresponds to a map of the energy state for each node at a given moment.

Moreover, the DSA is also used to dynamically adapt the network topology within the cluster to reduce the

energy consumed for communication; thus, extending the lifetime of the network while achieving an acceptable performance for data transmission [14].

The proposed framework hierarchically combines three security layers. At the bottom of this approach (Layer L1), an IPS-based authentication process is designed to provide a lightweight security scheme in the data plane. In the middle of the framework (Layer L2), an IDS-enabled energy prediction model within the edge is designed with the aim of supplying a cost-effective intrusion detection solution near the data plane.

Finally, at the top of this framework (Layer L3), in the control plane, a SMS-based SVM algorithm is introduced to achieve isolation, high performance, enhanced anomaly detection, and efficient mitigation by segregating malicious nodes over the SDWSNs. Since the SMS-based SVM algorithm has global visibility of the sensor network, it can see the correlations between true positives, which lets it filter out the

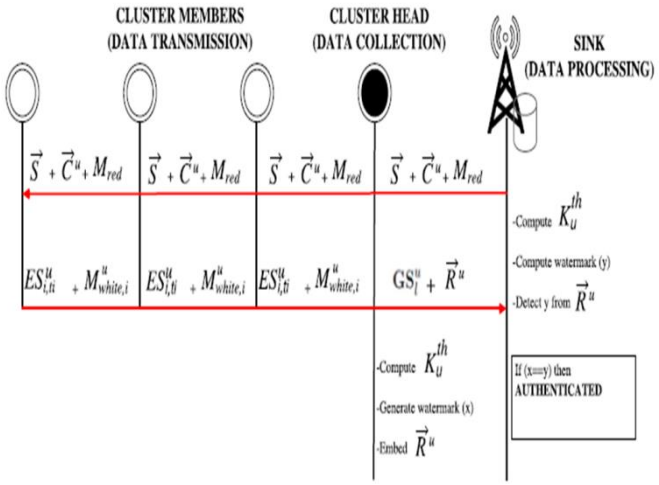


Fig. 3.2. DSA-based authentication and a watermarking technique.

false positives. Thus, the main contributions of this work are summarized as follows:

1) A novel security scheme based on network snapshot readings, providing continuous authentication in large-scale SDWSNs, is proposed.
2) A watermarking technique is exploited to guarantee the accuracy of concurrent authentications while performing data integrity checks for the entire SDWSN.
3) The authentication method is improved by introducing a link node, which creates a connection between all the clusters of sensors.
4) An edge computing empowered IDS is leveraged to efficiently handle the limited resources in SDWSNs.
5) A two label dataset is generated in the edge, with the aim to train an SVM classification algorithm that is subsequently used by the SMS; wherein the latter is deployed at the control plane and is designed to correlate the alerts from the low-delay IDSs distributed across the edge network.

Moreover, analysis of the computational complexity is provided and simulations showing the effectiveness of the proposed framework are executed by leveraging the AVISPA tool and The results demonstrate an accuracy of 84.75%.

XI. SYSTEM MODEL

Aiming to achieve high-security, address the limited resources constraints and take advantage of SDN architectures, our work proposes a collaborative security framework design, as depicted in Fig. 1a. To summarize, the proposed security framework possesses a hierarchical structure and comprises of three layers. At the bottom of the framework stack, in the data plane, in L1, an IPS-based authentication process is performed. At the middle, at the edge, in L2, an IDS-enabled energy prediction model is executed, and finally, in the control plane, in L3, the SMS-based SVM algorithm is designed. In this context, in L1, a cluster-based WSN is created [14] and DSA is employed, where the sink nodes initiate the snapshot acquisition process by sending a marker message to their cluster heads in order to form a global energy state of the network. Afterwards, the marker message

is propagated to the cluster members. Each member sends its energy state back to its cluster head post receiving the message. Once the cluster head collects the global energy state from its cluster members, it protects the data using a watermarking embedded method with the aid of a generated public key and other security parameters to ensure that the derived data will not be altered on the fly by possible malicious attackers. Consequently, the network snapshot and the watermarked data is forwarded to the sink node. Likewise, the sink sends a copy of the energy map to the control plane, which is located in the cloud. Moreover, in the edge, the sink node periodically receives the snapshot readings aiming to detect the embedded watermark for the sake of continuous authentication and for the subsequent energy consumption prediction procedure.

XII. REFERENCES

[1]. Jianguo Zhou; Hao Jiang; Jing Wu; Lihua Wu; Chunsheng Zhu; Wenxiang Li, Year: 2016,"SDN-Based Application Framework for Wireless Sensor and Actor Networks", IEEE Access, vol. 4, pp. 1583 – 1594.

[2]. Jun Wu; Kaoru Ota; Mianxiong Dong; Chunxiao Li, Year: 2016, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Access, vol. 4, pp. 416 – 424.

[3]. Israat Haque; Mohammad Nurujjaman; Janelle Harms; Nael Abu-Ghazaleh, Year: 2019,"SDSense: An Agile and Flexible SDN-Based Framework for Wireless Sensor Networks", IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1866 – 1876.

[4]. Bruno Trevizan de Oliveira; Lucas Batista Gabriel; Cintia Borges Margi, Year: 2015, "TinySDN: Enabling Multiple Controllers for Software-Defined Wireless Sensor Networks", IEEE Latin America Transactions, vol. 13, no. 11, pp. 3690 – 3696.

[5]. Christian Miranda; Georges Kaddoum; Elias Bou-Harb; Sahil Garg; Kuljeet Kaur, Year: 2020, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2602 – 2615.

[6]. Angelos-Christos G. Anadiotis; Sebastiano Milardo; Giacomo Morabito; Sergio Palazzo, Year: 2018, "Toward Unified Control of Networks of Switches and Sensors Through a Network Operating System", IEEE Internet of Things Journal, vol. 5, no. 2, pp. 895 – 904.

[7]. Lucia Lo Bello; Alfio Lombardo; Sebastiano Milardo; Gaetano Patti; Marco Reno, Year: 2020, "Experimental Assessments and Analysis of an SDN Framework to Integrate Mobility Management in Industrial Wireless Sensor Networks", IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5586 – 5595.

[8]. Alex Mavromatis; Carlos Colman-Meixner; Aloizio P. Silva;