A Survey on Authentication Schemes for Wireless Sensor Networks

Valentin-Alexandru VLĂDUȚĂ, Diana-Andreea ARSENE, Ana-Maria GHIMEȘ

***Abstract*—Nowadays, security is one of the main concerns in industry and academia. Complexity and number of attacks increased, which translates in higher vulnerability for end users and companies. Wireless sensors are one of the most vulnerable devices on the market due to their limited hardware and software capabilities. Attackers focus on these devices due to their limitations, with the end goal of compromising the entire workgroup or network. To counter this trend, developers and researchers started to propose different schemes and protocols that increase security. This paper has the goal of presenting a thorough analysis on existing authentication mechanisms in order to gain knowledge on the existing schemes, techniques, implementations and issues. Furthermore, with a thorough study, one can propose future implementations that may apply on different solutions.**

***Index Terms*—authentication, sensor systems and applications, wireless communication, wireless sensor networks.**

I. INTRODUCTION

Attacks on wireless sensors have increased in the recent period and the trend suggests that this will not stop, but accelerate. Authors of [1] reveal that attacks can occur on all layers (physical, link, network, transport and application). For this reason, creating a safe environment for these devices can become difficult due to the variety of attacks that can occur and to the limitations that are related to these devices.

Wireless sensor networks (WSNs) can be used in complex applications to monitor environmental parameters, track changes and control the method how the solution is working. Also, a sensor node has constraints at different levels: power, computation, storage and communication. All of these can be seen by attackers as a perfect entry point into an infrastructure. By attacking the weakest point in a network, one can gain access to more resources, even if, initially, only a sensor node was hacked. It only takes a weak point to be breached in order to compromise the entire network. Over the years, many attacks targeted IoT devices: temperature sensors in a fish tank led to a major data breach in a casino (according to [2]), a coffee machine infected an entire network with ransomware (according to [3]) or a household sensor led to a breach in the entire local network which translated into a leak of financial records.

V. A. Vlăduță is with the Doctoral School for Defense and Security Systems Engineering, Military Technical Academy, 39-49 George Coșbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: alexandru.vladuta@mta.ro).

D. A. Arsene is with the Faculty of Automatic Control and Computers, "Politehnica" University of Bucharest, 313 Independence Ave., Sector 6, 060042, Bucharest, Romania (e-mail: arsene.diana.andreea@gmail.com).

A. M. Ghimeș is with the Doctoral School for Defense and Security Systems Engineering, Military Technical Academy, 39-49 George Coșbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: ana.ghimes@mta.ro).

Regardless the type of sensor, they pose a security threat to any environment to which it has connectivity. For this reason, this topic is of interest for many research teams and industrials. A lot of effort has been deployed into securing Internet of Things (IoT) devices and a lot of work is still needed to reach the intended level of security for the current needs of an individual or organization.

The current paper proposes a study on authentication schemes for wireless sensors and their appliance in different scenarios. A review for existing technologies is made and a set of propositions on how to use certain technologies in a given set of environment conditions are also summarized in this paper.

The remaining of the paper is organized as follows: attacks and vulnerabilities are presented in Section II, authentication schemes are revealed in Section III, a proposition is summarized in Section IV and, finally, conclusions are drawn in Section V.

II. SENSOR VULNERABILITIES & ATTACKS

This section presents a series of vulnerabilities that are associated with wireless sensors along with attacks that are directed to exploit the specific vulnerability. With a deep understanding related to the cause, a solution can be then presented to solve some of the raised issues.

One of the vulnerabilities that are associated with wireless sensors is linked to the physical aspect. Due to their placement at different remote positions, they are exposed to many types of attacks. Tampering is one of the most effective attacks that can be deployed. An attacker can extract data from the sensor (encryption / decryption / authentication keys or data) or can modify information (routing scheme, network address, etc.) to change the role of the device from its initial state. Moreover, identity replication attacks may also be deployed if an attacker uses a configuration file from a tampered sensor on its own device. In [4-5], authors propose two different solutions for resisting to tampering attacks.

The power component is a limitation that is specific to wireless sensors. Due to their size and remote placement, the power capacity of sensors is limited. For this case, it is vital to use the available resources as efficiently as possible. There are several attacks that can affect directly the power capacity. The flood attack, exhaustion attack and replayed routing information attack are the most well-known types that affect directly the power consumption. If a sensor receives a high amount of data (flood/exhaustion) from an attacker, it will decrease its capacity a lot faster than other sensors in the area and will end up shutting down. Moreover, if a routing scheme is altered and traffic is

Digital Object Identifier 10.32754/JMT.2018.2.04

redirected to a certain node in order to overwhelm it, in the end it will also decrease its power sooner than other nodes. Two solutions to counter flood attacks are presented by authors of [6-7].

When referring to the computation power and storage, the two are also limited when referring to wireless sensors. The reduced size of sensors created limitations for the computation power and storage, increasing the effort made by developers to secure these devices. As in the previous case, flood attacks and replayed routing information attacks are also issues that affect computation power and storage.

Lastly, the communication component of a sensor may be susceptible to attacks. Jamming frequencies that are used by devices can prevent any communication between sensors and the WSN collapse. Different types of jamming attacks exist, based on the duration of the jamming signal: for a temporary period, intermittent or permanent. Solutions for this type of attack are presented in [8-9].

Many more vulnerabilities and attacks exist on wireless sensors, but the survey limited only on the ones that affect directly the sensor device. Other types, like sinkhole, wormhole, Sybil, selective forwarding were not presented into detail. They do not target a specific sensor, like the previously mentioned ones, but the communication between devices.

III. Authentication Schemes

This section focuses on presenting relevant work from different research teams that tackled with securing wireless sensors. With a deeper understanding upon the current development level, one can go further and propose a solution for a specific vulnerability or scenario that has not been taken into account by other research teams.

An approach for authenticating sensors is proposed in [10]. Authors claim that they were among the first to propose a scheme that uses concurrent secure connections. Devices have to run multiple instances of the protocol in order to assure the desired level of secureness. The protocol is formed out of two suites: a keying suite and an authentication suite. The keying suite is formed out of a key agreement protocol, a key retrieval protocol and a key management protocol, while the authentication suite is composed of a part for authenticating sensors to the sink, and a part for authenticating with the base station. Moreover, the protocol is intended for devices that are dynamic. More technical details can be reviewed in [10].

In [11] authors reveal that symmetric-key-based authentication (µTESLA) are inefficient and pose security threats for sensors due to the delayed authentication of the messages. The solution came from public key cryptography (PKC). Even if initial theories conclude public key cryptography is not suitable for WSN due to computational costs, recent studies demonstrated that PKC can be a solution if it is used only with software implementations. Results demonstrated that PKC schemes obtained the desired security level with minimized computational and communication costs. They tested three distinct approaches: Bloom filter scheme, partial message recovery signature scheme and Merkle has three.

Another approach is presented in [12], where authors reveal the implementation of IBE-Trust protocol on actual sensor boards and test its performance. The theoretical presentation was detailed in a previously published paper [13]. IBE-Trust is an identity-based authentication protocol that assures all major security aspects (confidentiality, integrity and authenticity). It is formed out of 2 phases. In pre-deployment sensors are prepared offline, before joining the network, by generating global system parameters and public key. Moreover, the base station creates a trust list with all sensors that are present in the network. In the deployment stage, encrypted data (with the public key) is exchanged between sensors and the base station in order to validate the identity and ensure the trust between entities. The base station decrypts the received data and verifies the identity with the entries in its trust list. If it is in the list, the base station responds with an acknowledgement and informs neighboring members that a new device is trusted, otherwise it discards the packet. The solution was tested on two XBee devices and results in terms of energy efficiency look promising. Furthermore, authors reveal that the solution can be applied with success in e-Health applications.

The proposition from [14] is formed out of two phases also. In the first one (Registration Phase) security credentials are obtained from a trusted parted, while in the second one (Authentication Phase) the actual communication between the two devices begins with the credentials previously obtained. The authentication is done with the aid of elliptic curve cryptography (ECC) and assigns a high level of security due to the PKC. Moreover, in the first phase the authenticator analyzes the hello messages initiated by applicants and in this manner Denial of Service (DoS) attacks are prevents. Data integrity is ensured by the fact that the exchanged messages contain message authentication codes (MAC). It is very important that sensors are physically protected so that attackers do not get the opportunity to access them and extract public/private keys information that can compromise the entire network.

Authors of [15] propose a solution named PAuthKey protocol. It is formed out of two phases, as most existing protocols: registration phase and authentication phase. During registration, each sensor from a cluster should obtain a certificate from the cluster head (CH) and form its own public-private key pair from the certificate. The authentication method varies and reaches to a total of three types: authentication between two sensors in the same cluster, authentication between sensors in different clusters and authentication between sensors and end-users. This approach is different from other propositions and may be considered a starting point for future proposals. Finally, tests were made with TelosB sensor nodes and results reveal a high level of security against attacks.

A proposal that was tested using OMNET++ simulator is presented in [16]. Authors reveal a scheme that reduces memory overhead by using on-line key generation method based on ECC. The network has three types of nodes: a base station, cluster heads and sensors. Cluster heads are also sensors but with increased computational capabilities. The base station will act as a trusted party, while cluster heads are directly authenticated by the base station and will have the roll to authenticate the sensors in their cluster. The proposition has 5 phases: key pre-distribution, cluster head authentication, cluster formation, sensor authentication and,

finally, key establishment/management. ECC is used to generate public/private key pairs for the authentication process between base station and cluster heads. Clusters are formed based on the received signal strength and with the condition that cluster heads are aware of all neighbors of each sensor in their cluster. Moreover, data broadcasted by the cluster head is encrypted and only sensors that are able to decrypt and respond get authenticated by the cluster head. The initial keys are generated and inserted into devices before deployment. Moreover, for secret key generation, each cluster head uses the prime numbers of the devices to which it wants to communicate to along with its own prime number. This approach can be used for further proposal, due to the method of generating secret keys based on information received from neighboring devices.

A different approach from the rest is described in [17]. The novelty in the proposition resides in the anonymization of users that connect to the WSN. The proposition uses dynamic identification technique. Users obtain encoded dynamic entities from their real entities in order to protect them from potential attackers. Moreover, user information cannot be revealed without the secret key. After each successful session, a randomly generated pseudonym is created for both the user and the network gateway. Given that this pseudonym is changing at each session, the attacker cannot track a particular user. One limitation exists for the current proposition and is bounded to synchronization attacks. This solution can also be implemented in a future proposition and is of interest for many other fields and applications in which user information is sensitive.

Authors of [18] focus on presenting a solution that uses both data aggregation and authentication for securing data. Sensors are divided into clusters and each cluster head has the role to aggregate data and forward it to the sink. The novelty of this approach is that each node slices its information and broadcasts it to its neighbors while encrypting it with a key that is specific to the communication to each neighbor. Moreover, each node collects slices for a fixed amount of time and at the end it forwards data to the aggregator that will also forward it to the sink. Moreover, simulations were done with the aid of Network Simulator 2 and results reveal that the solution can represent a viable securing method.

Finally, in [19] is revealed an authentication mechanism that uses two level authentication to filter potential attackers and secure even more the sensor network. The first authentication layer is done by sensors with increased features that receive request from ordinary sensors. Only if the request passes this level, it gets forwarded to the base station for a final validation and approval. The first layer authenticators have the role of cluster heads also. In order to reach the base station, cluster heads forward from one to another until data reaches the destination. Authors used a WSN formed out of Mica2 sensor nodes to test the implementation. Authors also mention that this solution overcomes limitations found in other existing protocols (SPIN or BROSK). For further details and results, one can review information in [19].

After reviewing existing wireless sensor network authentication protocols, one can observe that some research teams focused on developing and testing solutions for hardware devices (different sensor boards), while others focused on creating models in simulators (different platforms). Depending on the scenario and scenario pre-requisites, each proposition has its benefits and limitations.

IV. AUTHENTICATION PROPOSITION

This section focuses on presenting a proposition for a communication protocol that has no security features. In the initial version, communication is established between a dynamic unmanned aerial vehicle (UAV) and static sensors. The UAV advertises its GPS position regularly and receiving sensors start a prioritization process based on the received information and own data with the end goal of preventing collisions in the communication process. More details can be found in [20].

Due to the increased number of attacks and to the vulnerabilities specific to IoT devices, we considered including security features into communication as vital. For this reason, we started by reviewing existing work, to pin place the position of recent novelty in the field. We then shifted on extracting relevant data from propositions and creating our own method for authenticating information based on the requirements of the scenario. After a proposition is modeled, as future work we intend to implement and compare results with similar schemes in order to test its efficiency from different points of view (energy efficiency, scalability, resistance to different types of attacks, etc.).

After reviewing papers that relate to authentication schemes in WSN, one can conclude that most implementation have a pre-deployment phase in which devices are prepared. Certain keys or nonces are pre-uploaded for the authentication process. Therefore, we will use this part also and consider uploading some pre-shared keys in the devices.

In our scenario, the UAV communicates with each sensor on the ground and collects its data. For this reason, we will consider authenticating each sensor before collecting data. The UAV will be considered legitimate and not be authenticated by sensors. Furthermore, if a certain pattern of packets are not exchanged between the UAV and a sensor, the data communication does not start. For this reason, it is not so easy to replicate the role of the UAV by a potential attacker. The authentication will use the pre-shared keys from the pre-deployment phase, along with a set of nonces in order to to prevent replay attacks. Furthermore, secret keys are generated every time communication is established between the two devices, to keep communication freshness.

An extra security measure will be in the form of authentication between sensors. Even if they do not transfer data between them, some of the sensors will be deployed with a double role. One, as a regular sensor to collect data and the other, as a security enforcer, to check the identity of its neighbors in order to pre-filter potential attackers before the UAV arrives at the location to start the gathering process. These sensors will build blacklists and will be forwarded to UAVs to prevent any potential attacker from sending false data or flooding the collector with packets in order to prevent legitimate sensors from sending their data.

The implementation of [20] was made in Network Simulator 2 and the security features will also be included in

the same project. Finally, in order to fairly test results, one should consider similar propositions that are also implemented in simulators and not compare with results from real testbeds. Therefore, using results from [16] and [18] for comparison would be a good approach on testing the efficiency of the proposition.

V. CONCLUSIONS

The number of attacks that target wireless sensors has increased in the past few years due to their vulnerability given by their limited hardware and software capabilities. Many studies were conducted in this area and motivated industrials and academia to focus on developing lightweight protocols and schemes to counter this trend.

This paper had the objective of shaping the context related to authentication in wireless sensor networks in order to observe the exact development state in the field and to find what advantages can be taken from existing project and how to improve certain limitations with the end goal of developing a solution that is intended for data collection with the aid of unmanned aerial vehicles. After identifying vulnerabilities that are related to sensors and common attacks, the attention moved on reviewing existing protocols. Regardless the platform, either simulator or on real test beds, authors propose solutions for different types of attacks, on different scenario requirements. Starting from these, we extracted what can fit our scenario requirements (simulator with data collection made from a mobile UAV) and proposed a solution that we plan to develop in the near future as part of an existing project in Network Simulator 2.

As future work, we intend to implement, beside the scheme in the simulator, a solution on a real test bed with static Memsic sensors (MIB520 base station, MDA100 sensor board and MICAz wireless system) that are placed at various locations on the ground and a mobile UAV from DJI (Matrice 100) that will collect data from them. We have already tested the data collection process with these pieces of equipment, without any security features, and plan to further extend this project as well.

REFERENCES

[1] R. Singh, J. Singh, and R. Singh, "Attacks in Wireless Sensor Networks: A Survey," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 5, pp. 10-16, May. 2016.

[2] Liquid IT, Security Bulletin, May 2018, [Online]. Available: https://liquidit.nz/wp-content/uploads/2017/09/Liquid-Security-Bulletin-May-2018.pdf

[3] M. Polychronakis, CSE Network Security, November 2018, [Online]. Available:https://www3.cs.stonybrook.edu/~mikepo/CSE508/2017/lectures/CSE508_2017_lecture_19_privacy.pdf

[4] L. Xie, H. Zhu, Y. Xu and Y. Zhu, "A Tamper-resistance Key Pre-distribution Scheme for Wireless Sensor Networks," in Proc *Fifth Int. Conf. on Grid and Cooperative Computing Workshops*, Hunan, China, Oct. 2006, pp. 437-443. doi:10.1109/GCCW.2006.13

[5] J. Bian, R. Seker, S. Ramaswamy, and N. Yilmazer, "Container communities: Anti-tampering Wireless Sensor Network for global cargo security," in Proc. *17th Mediterranean Conference on Control and Automation*, 2009, pp. 464-468. doi:10.1109/MED.2009.5164585

[6] K. Saghar, D. Kendall, and A. Bouridane, "RAEED: A solution for hello flood attack," in Proc. *12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Islamabad, Pakistan, Jan. 2015, pp. 248-253. doi:10.1109/IBCAST.2015.7058512

[7] V. Nigam, S. Jain, and K. Burse, "Profile Based Scheme against DDoS Attack in WSN," in Proc. *Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, India, 2014, pp. 112-116. doi:10.1109/CSNT.2014.31

[8] Y. Ettouijri and Y. Salih-Alj, "Countermeasures against energy-efficient jamming on wireless sensor networks," *2014 International Conference on Multimedia Computing and Systems (ICMCS)*, 2014, pp. 916-920. doi:10.1109/ICMCS.2014.6911262

[9] A. Ghosal, S. Halder, M. Mobashir, R. K. Saraogi, and S. DasBit, "A jamming defending data-forwarding scheme for delay sensitive applications in WSN," *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, Chennai, India, 2011, pp. 1-5. doi:10.1109/WIRELESSVITAE.2011.5940919

[10] M. Bilal and S.-G. Kang, "An Authentication Protocol for Future Sensor Networks," *Sensors*, 2017, vol. 17, no. 979. doi:10.3390/s17050979

[11] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4554-4564, Oct. 2009. doi:10.1109/TVT.2009.2019663

[12] Y. M. Yussoff, N. H. Kamarudin, and H. Hashim, "Lightweight Trusted Authentication Protocol for Wireless Sensor Network (WSN)," *International Journal of Communications*, vol. 2, pp. 130-136, 2017.

[13] Y. M. Yussoff, H. Hashim, and U. T. Mara, "IBE-Trust: A Security Framework for Wireless Sensor Networks," *World Congress Internet Security (WorldCIS)*, London, UK, 2011, pp. 171-176.

[14] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, Istanbul, Turkey, 2014, pp. 2728-2733. doi:10.1109/WCNC.2014.6952860

[15] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M.Ylianttila, "PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," *International Journal of Distributed Sensor Networks*, 2014, vol. 10, no. 7, doi:10.1155/2014/357430

[16] S. U. Khan and R. Khan, "An Efficient Authentication and Key Establishment Scheme for Heterogeneous Sensor Networks," in *Proc. 2011 7th International Conference on Emerging Technologies (ICET)*, Islamabad, Pakistan, doi:10.1109/ICET.2011.6048451

[17] L. Xiong, D. Peng, T. Peng, H. Liang, and Z. Liu, "A Lightweight Anonymous Authentication Protocol with Perfect Forward Secrecy for Wireless Sensor Networks," *Sensors*, vol. 17, no. 11, Nov. 2017, doi:10.3390/s17112681

[18] V. Bhoopathy and R. M. S. Parvathi, "Secure Authentication Technique for Data Aggregation in Wireless Sensor Networks," *Journal of Computer Science*, vol. 8, no. 2, pp. 232-238, 2012.

[19] R. Riaz, T.-S. Chung, S. S. Rizvi, and N. Yaqub, "BAS: The Biphase Authentication Scheme for Wireless Sensor Networks," *Hindawi Security and Communication Networks*, vol. 2017, 2017. doi:10.1155/2017/7041381

[20] A.-V. Vlăduță, M. L. Pura, and I. Bica, "MAC Protocol for Data Gathering in Wireless Sensor Networks with the Aid of Unmanned Aerial Vehicles," *AECE Journal*, vol. 16, no. 2, May 2016, pp. 51-56, doi:10.4316/AECE.2016.02007