PAPER

Real-Time Monitoring Systems That Provide M2M Communication between Machines

Ya ZHONG[†a)], ***Nonmember***

SUMMARY Artificial intelligence and the introduction of Internet of Things technologies have benefited from technological advances and new automated computer system technologies. Eventually, it is now possible to integrate them into a single offline industrial system. This is accomplished through machine-to-machine communication, which eliminates the human factor. The purpose of this article is to examine security systems for machine-to-machine communication systems that rely on identification and authentication algorithms for real-time monitoring. The article investigates security methods for quickly resolving data processing issues by using the Security operations Center's main machine to identify and authenticate devices from 19 different machines. The results indicate that when machines are running offline and performing various tasks, they can be exposed to data leaks and malware attacks by both the individual machine and the system as a whole. The study looks at the operation of 19 computers, 7 of which were subjected to data leakage and malware attacks. AnyLogic software is used to create visual representations of the results using wireless networks and algorithms based on previously processed methods. The W76S is used as a protective element within intelligent sensors due to its built-in memory protection. For 4 machines, the data leakage time with malware attacks was 70 s. For 10 machines, the duration was 150 s with 3 attacks. Machine 15 had the longest attack duration, lasting 190 s and involving 6 malware attacks, while machine 19 had the shortest attack duration, lasting 200 s and involving 7 malware attacks. The highest numbers indicated that attempting to hack a system increased the risk of damaging a device, potentially resulting in the entire system with connected devices failing. Thus, illegal attacks by attackers using malware may be identified over time, and data processing effects can be prevented by intelligent control. The results reveal that applying identification and authentication methods using a protocol increases cyber-physical system security while also allowing real-time monitoring of offline system security.

key words: *machine-to-machine communication, trust, wireless systems, offline operation, data transmission, Internet of Things, intelligent control*

1. Introduction

Machine-to-machine (M2M) communication networks open up new possibilities for developing and implementing multifunctional user applications without the need for human intervention. This allows for remote monitoring through the use of communications and hardware. Due to the limited resources available to machines and auxiliary devices in M2M communication networks during operation, some limitations apply. Electricity, bandwidth, storage, and complex calculations are examples of such limitations. With such limitations, issues arise when designing networks for M2M communications and pose a threat to the security and confidentiality of data stored on cloud servers [1]. This emphasises the importance of researching potential threats that may exist in M2M systems and resolving them using newer and appropriate solutions [2]. M2M communications allow data to be exchanged using a communication system that links a set of sensors, a wireless network, and a computer with Internet access [3]. The term M2M is linked to the Internet of Things, in which electronic devices are linked via intelligent networks via a wireless communication channel [4]. M2M networks can use a variety of communication technologies such as cellular GSM, Wi-Fi, GPRS, EDGE, 4G, ZigBee, and others as communication channels for receiving and processing data. In the energy sector, ZigBee and M2M interconnections are used, for example, to control the management of solar and wind power plants [3], [5].

Sensors and other intelligent devices provide data from traditional computer networks. Security and data processing centres that deal with IT technologies are usually where these types of data are typically processed. The data volume of these can range from a few kilobytes to several megabytes [6]. There are numerous uses for the data generated by M2M devices in a variety of industries. They extract data via user applications that must adhere to security and privacy policies to avoid negative scenarios as a result of intruders' malware software attempts [3], [7].

1.1 Literature Review

The article [8] describes how to implement two-way authentication in the Internet of Things via a scheme based on existing Internet standards, protocols, and encryption algorithms such as RSA (6LoWPAN). Today, they are widely used in power-efficient wireless networks [9]. Using signature schemes and block encryption algorithms, the transmission model [10] satisfies the security requirements for anonymity and confidentiality of devices equipped with smart technologies (Internet of Things). Confidentiality and integrity in [11] are described as an existing management system key that is used to support modern M2M communications. The user authentication scheme and session key mutual agreement for WSN and M2M, which is proposed in [12], allows for secure session key negotiation between sensor nodes and the network. The main challenge is that identifying users for the desired access and control requires complex computational procedures that consume a lot of resources and power from the user node [13]. Access control for nodes responsible for data collection is one of the ac-

Manuscript received May 1, 2023.
Manuscript revised August 2, 2023.
Manuscript publicized October 17, 2023.

[†]The author is with Department of Information Engineering, Tongren Polytechnic College, Tongren, China.
a) E-mail: yazhong73@outlook.com

DOI: 10.1587/transfun.2023EAP1049

companying identification problems, as described in [14]. The authors devised a scheme for accepting and employing limited resources that allowed for the creation of only one encrypted key per user node. The identification system for emergencies resulting from M2M communications [15] is comprised of a registration process, user authentication, and a privacy policy. It can restrict access to data and information for legitimate users based on the severity of an emergency. The structure of the security archive is described in [16], which employs a prototype request processing mechanism for processed data streams that ensures data integrity and effectively provides data confidentiality.

A trust score is an important parameter in M2M communications during offline operation. The articles [17], [18] assess the level of trust that Internet of Things objects have. Objects are smart devices that use smart technologies and are connected to a wireless network with heterogeneous characteristics that allow an object to interact in a shared system. To prevent hostile software attacks, the objects are based on trust characteristics, which are algorithms with keywords and encryption algorithms [19]. There are two nodes in the dynamic distributed trust management protocol [20] that meet and complete the transaction at a single common point in time. After that, data exchange between nodes is used to evaluate the quality of their interactions. This means that evaluation and comparison are done for other nodes with which an intersection was possible. The social network concept developed in [21] introduces intelligent devices that can form social relationships among themselves, posing a social threat in the shared M2M communication system.

1.2 Problem Statement

The important problem is the modern development of wireless technologies with the use of M2M communication and intelligent devices for processing and recording data during offline operations, which are at risk of security due to the introduction and penetration of malware into the shared M2M monitoring system.

The purpose is to study security systems for M2M communication systems that require real-time monitoring based on the use of identification and authentication algorithms.

The objectives are:
- an analysis of the applications of M2M communication technologies, including their advantages and prospects;
- research on identification and authentication algorithms to ensure the safe operation of wireless technologies;
- research on the compatibility of identification and authentication algorithms in a shared system;
- an analysis of the advantages and prospects of using M2M communication for industrial purposes;
- research on the classification algorithm for M2M communication; and
- analysis and study of trust assessment and its parameters in M2M communications during offline operations.

The experimental part of this study aims to develop a methodology for managing, controlling, and monitoring system resources by simulating unauthorised access by malware and performing the necessary processes.

The academic novelty of this article is that it examines the methods and parameters of M2M security using wireless technologies, with an emphasis on the use of algorithms for identifying and authenticating intelligent devices for real-time monitoring.

The implementation limitations are that the M2M communication is studied in a connected system visually and using software via WSN wireless networks for conducting experiments involving intelligent devices and M2M communication.

2. Materials and Methods

The purpose of this article is to investigate methods for identifying, classifying, and authenticating intelligent devices and computers using protocols based on computational algorithms. These are based on wireless networks and allow for real-time system monitoring. AnyLogic software is used to create visual representations of the results using wireless networks and algorithms based on previously processed methods. We chose the Anylogic Simulation software because it is a leading simulation software for industrial and business applications, utilized by over 40% of fortune 100 companies today (https://www.anylogic.com). The W76S is used as a protective element within intelligent sensors due to its built-in memory protection.

2.1 Device Identification

Clustering is done offline to determine which node is the cluster head (CH) and which node is a cluster member (CM). Following that, nodes are classified as genuine or attacked devices based on the characteristics of a trust score in order to optimize the clustering process. Using these weighting values, a trust-score value ranging from 0 to 1 is computed.

Nodes are classified as authentic or attacked based on their trust-score value. Attacked devices update the CM list, whereas legitimate devices update the CH list. To compute the CH for a particular interval, the trust-score value of each node in the CH list is calculated on a periodic interval. The data transmission time interval is advertised and announced by the designated CH. At each interval, the remaining energy for the CH is checked, and the cluster cycle is modified correspondingly [22]. In M2M communications, identification and classification protocols are used to identify and classify devices. These involve a large number of intelligent devices that can communicate and interact with one another without the need for human intervention by receiving data. The Efficient Device Type Detection and Classification (EDDC) protocol [23] is one of these protocols that has been developed. The protocol is based on determining the type of device and includes an identification step that calculates each node's periodic trust-score value. The Trust Score (TS) is computed and identified first. The node is identified as an unidentified device if its TS value is greater than the global trust-score threshold value. In another scenario, the node can be identified as an attacked device.

A method for calculating the trust score has been developed to identify legitimate devices or possible malware attacks on nodes. It is based on the use of three main parameters when each node's periodic value is calculated. Successful Packet Delivery (SPD), Energy Level (EL), and Node Degree (ND) are among the metrics chosen as reliable indicators of malware behaviour and the consequences of a malware attack. In algorithm 1 [23] TS^n obtains the trust score n and calculates the trust scores using these three parameters.

In the event of a malware attack, the SPD is a vulnerable node. It takes on a malicious task and ensures that the network runs smoothly. Through this node, data is exchanged with other nodes and this node can figure out the SPD trust score for each device. The SPD node is calculated as follows [23]–[25]:

$$SPD^n = \frac{n^{rcv(t-1,t)}}{n^{ge(t-1,t)}} \tag{1}$$

where $n^{rcv(t-1,t)}$ and $n^{ge(t-1,t)}$ are the total number of data packets received and generated in the time interval from $t-1$ to t. Nodes with higher SPD values are more likely to be identified as unidentified (legitimate) devices.

The EL trust is determined in the nodes that consume energy faster while also acting as recommended parameters for data transmission or CH selection. These nodes can also be interpreted as malicious. It is necessary to calculate the trust score reliably by each device's current level of remaining energy:

$$EL = \frac{E_{rem}(n^t)}{E_i(n)}, \tag{2}$$

where $E_{rem}(n^t)$ is the remaining energy at a certain time t, and the value $E_i(n)$ is the initial energy level. If the node contains extremely high EL values, in this case, it is more likely to be identified as a legitimate device.

A malicious attack using software, eavesdropping, or data leakage can attract the source of information with false statements sufficient for neighbouring devices to send information a short geographical distance to the destination. The number of neighbours NC of node n at time t is calculated using $RSSI$:

$$NC = count\left[\frac{n}{distance(n, pi)} < RSSI\right], \tag{3}$$

where $n \neq pi$ and distance (n, pi) calculates the distance to the location of n and $pi^{th} \in N$, using $RSSI$ for n. NC is used to calculate the trust-score value and is calculated using the formula:

$$ND^n = 1 - \left(\frac{1}{NC}\right) \tag{4}$$

The number of closest or single nodes to the present node under examination, n, is computed in the following equation. This is accomplished by examining the RSSI boundaries, i.e. the distance between the present node n and its nearest node pi must be less than the RSSI value of the node under consideration. The count parameter reflects the total number of NC nodes that match the RSSI criterion and are regarded the closest nodes to the node n under investigation at the time. A weighted technique is used to determine node n's ultimate trust-score value:

$$TS = \left(\omega^1 SPD^n\right) + \left(\omega^2 EL^n\right) + \left(\omega^3 ND^n\right), \tag{5}$$

where the values w^1, w^2 and w^3 are chosen as 0.5, 0.4, and 0.4, respectively, so that the sum is 1.

2.2 Device Classification

Following the identification algorithm, device input and data input for the classification of devices are the next steps. It is shown in Algorithm 2 [23]. It uses a trust-score value that is calculated regularly, with each sensor node being identified and accepted by legitimate devices and nodes that are vulnerable to malware attacks. The trust score must be calculated for each node in the network using the data delivery and receipt coefficient. Additionally, the available energy is calculated, and the number of neighbours is identified.

To begin the classification process, clusters composed of a CH and CMs must first be classified. Legitimate nodes are considered for further CH selection, while malware-infected nodes serve as CMs. For each node, a trust score is calculated. The CH in the network is then chosen based on the trust-score value. The CH indicates the maximum energy consumption because it must be active at all times during the data transfer process [23], [26].

2.3 Device Authentication

An intelligent sensor with a protected element W76S (SE) and a 4-megabyte protected memory element W76F are examples of such devices (Fig. 1), as is a router with a Trusted Platform Module (TPM). Based on [27], the suggested system consists of two procedures: a) the registration procedure, in which the sensor registers with the Authentication Server (AS), and b) the authentication procedure, in which the sensor and the router are mutually authenticated [28].

There is a 4-megabyte W75F protected memory element that is part of the W76S protected element. This memory can be expanded to meet specific needs. The W76S is a 32-bit computer with a Reduced Instruction Set (RISC). It has a Memory Protection Unit and a core clock frequency of up to 100 MHz (MPU). W76S employs a variety of cryptographic coprocessors, including 3DES, AES 128/192/256, RSA-2048/4096, and ECC 521, as well as True RNG and Side-Channel Attacks (SCA). It can also be used for Embedded Universal Integrated Circuit (eUICC) applications, which support multi-purpose, remote provi-

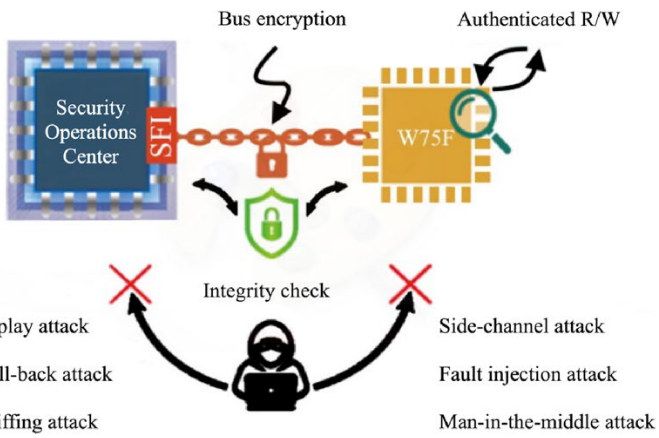

Fig. 1 W76S protected element with 4-megabyte W76F protected memory element.

sioning, and improve the M2M ecosystem's operational efficiency [27], [29].

The W75F Secure Flash Solution is the first secure flash memory device to be Common Criteria (CC) EAL5+ certified. The W75F memory element protects the confidentiality and integrity of data code in the Internet of Things devices and M2M communications by providing eXecute-in-Place (XiP) security.

Universal Integrated Circuit Card (UICC), integrated security element, artificial intelligence (AI) platforms, and integrated Hardware Security Modules (HSM) for automotive subsystems are some examples of use cases.

The W75F secure memory element provides the safest external code and data storage. This is a safe way to process connected devices that want to keep their products safe from threats like replay, rollback, attacker-in-the-middle attacks, sniffing, side channels and error injection.

The processes of device registration and authentication are following: x is a secret key protected by AS; PSK is a secure pre-key between AS and router; ID_i is the identification of intelligent sensor i; AID_i is the alias of an object I; F^i is the formation of functions; Sk_i is a shared key between intelligent sensor i and *TPM router; R^i* is a random number generated by a pseudorandom number generator; $h(.)$ is a one-way hash function; $\|$ is the concatenation operator; $\oplus$ is the XOR operation [27].

AS generates a secure set of pre-keys $\mathrm{PSK_i}$, $i = 1, \ldots, n$ and sends each PSK_i to a router.

1) Intelligent sensor → AS;

$$2)\ f_{1i} = h(ID_i\|x),\ f_{2i} = h\left(f_{1i}\right),\ f_{3i} = PSK \oplus f_{1i} \tag{6}$$

the purpose of f_{1i}, f_{2i} is to build a connection between the sensor ID and AS

3) AS → smart sensor [27].

After registration, the router authenticates each sensor. The sensor does not use real data for authorisation on the router during the authentication procedure. Thus, an attacker cannot overhear the smart sensor's ID. The steps involved in the authentication process are:

1) The intelligent sensor generates a random number R_i and stores it in the protected element W76S of the sensor, after which the parameter M1 is calculated as follows:

$$M_1 = h\left(f_{2i}\right) \oplus R_i \tag{7}$$

After that, the sensor calculates aliases as:

$$AID_i = h\left(R_1\right) \oplus ID_i \tag{8}$$

and calculates the parameter M_2:

$$M_2 = h\left(R_i \|M_1\| AID_i\right) \tag{9}$$

2) Smart sensor → router_I,

3) After receiving the authentication request, the router performs the following actions:

- the router extracts f_{1i} using a pre-shared PSK key $f_{1i} = f_{3i} \oplus PSK$
- then the router gets R_1 and ID_i for the formula:

$$R_i = M_1 \oplus h\left(f_{2i}\right) \text{ and } ID_i = AID_i \oplus h\left(R_i\right) \tag{10}$$

- then router_i calculates whether the $h\left(R_i \|M_1\| AID_i\right)$ value is equal to M_2 where the authentication request is rejected if $h\left(R_i \|M_1\| AID_i\right)$ and M_2 are not the same.
- next, the router generates a random number R_2, which is stored in the router's TPM, then it calculates AID_j, M'_1 and M'_2 by formulas:

$$AID_j = R_2 \oplus h\left(ID_i\right) \tag{11}$$

$$M'_1 = f_{1i} \oplus h\left(ID_i\right) \tag{12}$$

$$M'_2 = h\left(M'_1 \left\|AID_j\right\| R_2\right) \tag{13}$$

- finally, the router calculates the session key $\mathrm{SK_{ij}}$ by the formula:

$$SK_{ij} = h\left(R_i \| R_2\right) \tag{14}$$

4) $\mathrm{Router_i}$ → intelligent sensor, where the router sends back to the sensor an authentication response (message 4), including M'_1, M'_2 and AID_j.

5) The intelligent sensor extracts R_2 according to the

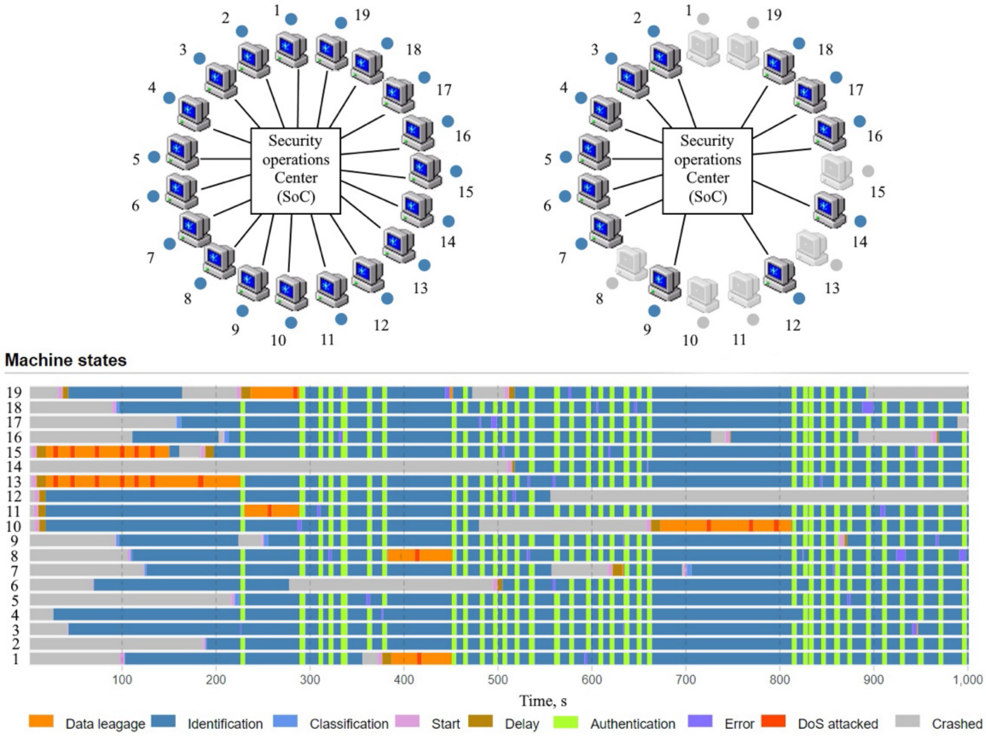

Fig. 2 M2M communication monitoring systems and states in different conditions.

formulas:

$$AID_j \oplus h\,(ID_i) \tag{15}$$

$$h\left(R_2 \,\|M_1'\|\, AID_j\right) \tag{16}$$

If they are equal, the router calculates the session key SK_{ij} using the formula (16).

Finally, the intelligent sensor calculates M_1'' by the formula:

$$SK_{ij} \oplus h\,(R_2) \tag{17}$$

6) Smart sensor → router, where the smart sensor sends a message 5 that includes M_1'' router$_i$.

7) After receiving message 5, the router uses its session key SK_{ij} calculated in step 3 to receive $h(R_2)$. The router then calculates $SK_{ij} \oplus M_1''$ and compares it with the value $h(R_2)$. If they are equal, it means that the intelligent sensor owns a legitimate session key [27]–[29].

3. Results

This article examines the M2M communication relationship, which is based on intelligent sensors and machines that are connected to a shared system in real-time and operate offline. Using AnyLogic software simulation, the main computer of the security operations centre is monitored. The M2M communication control structure consists of 19 machines, numbered from 1 to 19. Each machine includes an M2M server, main network, M2M network, and sensors. M2M servers are connected between each other, and each machine is connected with Security Operations Centre (SoC). Moreover, it contains a data set derived from data collected by intelligent sensors on computers under the control of the Security Operations Centre (SoC).

Data from smart sensors helped figure out the state and interaction of machines in different work processes in Fig. 2. Processes such as identification, classification, and authentication are examples. If the machines are operating in offline mode, they begin at the starting point (shown in pink), and their final operation is the crash condition (shown in grey), after which they can restart automatically and continue operating. Data leakage occurs when attackers use malware to try to break into the system.

Machine startup and authentication, which ensures the machines' safety and data storage, cause M2M communication delays. In some cases, attackers can get around the authentication process, which can harm the performance of the machine and the system as a whole. Additional authentication is required after that. Complex verification algorithms are linked to errors that most commonly occur during the authentication process. These are based on the use of algebraic formulas and encryption algorithms, which can result in errors if a machine runs incorrectly during data processing. A denial-of-service (DoS) attack is a malware-based hacker attack on a computer system that results in system failure and crash.

Figure 2 shows two identical 19-machine circuits. Of these, one depicts the system's active state of operation in the shared SoC environment. The other chart shows machines that became disabled as a result of data leakage and

Table 1 Results of machine malware attacks.

Machine number	Attack duration, s	Attack quantity
1	70 (380-450)	1
8	70 (380-450)	1
10	150 (650-800)	3
11	70 (220-290)	1
13	200	7
15	190	6
19	70 (220-290)	1

malware attacks. Due to the offline operation, the machine state tracking process is a chart of 19 machines that have been subjected to various processes and unwanted failures over time.

Machines 13 and 15 are exposed to system hacking and data leakage for 200 s, as shown in Fig. 2, resulting in the early authentication of all machines in the system for data security and confidentiality. Fig. 2 shows that the attacks lasted 200 s, with multiple attacks on the computer system. Machine 13 was subjected to 7 attack attempts, while machine 19 was subjected to 6. Each unexpected malware attack triggered an authentication process. Machines 11 and 19 were subjected to a brief data leakage attack between 200 and 300 s at the beginning of the authentication process. Similarly, machines 1 and 8 were re-authenticated between 400 and 450 s, which caused them to have a short data leak. Machine 10, which had failed as a result of the operation, had been subjected to a brief malware attack 3 times between 660 and 800 s after restarting the system, resulting in data leakage.

Table 1 summarises the test results of the machines in the shared system during offline operation.

The table shows that data leakage with malware attacks lasts 70 s for 4 machines. The duration for 10 machines is 150 s, with 3 attacks. Machine 15 had the longest attack duration, lasting 190 s and involving 6 malware attacks, while machine 19 had the shortest attack duration, lasting 200 s and involving 7 malware attacks. The highest numbers indicate that attempting to hack a system increases the risk of damaging a device, potentially resulting in the entire system with connected devices failing.

4. Discussion

Year after year, the rate of technological advancement in computer software applications continues to accelerate. This suggests that wireless technology is also improving. Moreover, it has a wide range of applications:
- various machine learning models and schemes;
- the Internet of Things;
- communication networks based on the interaction of various intelligent sensors and the use of M2M communication.

Existing knowledge and academic publications about this subject help make sure that the appropriate equipment is safe to use. This, in turn, enables the national level of safety to be raised. People use a lot of different protocols that use computational logarithms to make machines run more efficiently and keep them safe. These can make sure that all the machines work together well in a single monitoring and control system [3]–[11].

The use of an authentication scheme for M2M communication systems in a shared cyber-physical system in operation [30], [31] with support for intelligent devices based on the Internet of Things is one possible solution for increasing efficiency. To increase security, the scheme allows any pair of objects in the M2M network to mutually authenticate each other and agree on a session key for data transmission. It requires the user to possess only one secret key, which the M2M service provider can supply. With it, the user can navigate freely through the M2M network and authenticate at any of the domain's gateways. The authentication scheme does not rely on complex computational processes or cryptographic operations with a public key. In contrast, authentication is accomplished through the use of symmetric key encryption and a small number of hash accesses. The scheme, on the other hand, is better suited to devices with limited computing and storage resources. The presence of ineffective protective elements in the scheme accounts for this.

The research [32] identifies known optimization issues and provides a scalable priority-based resource allocation system for M2M communication in the LTE/LTE-Advance network. The resource allocation system provided finds a compromise between resource usage and application priority support. The suggested scheduling algorithm surpasses the usual algorithms in terms of resource sharing fairness, average resource usage, QCI priority support, and delay budget violation, according to the results.

The authors of [28] propose an improved M2M authentication protocol that could be used offline. It enables a high level of security as well as a high data exchange rate. The increase in computing load and communication overhead costs are unaffected by this protocol. This, in turn, ensures data storage when mutual authentication is achieved, the session key is negotiated, and the confidentiality of device identification data is increased for better resistance to various attacks. The protocol development process is divided into three phases: registration, key negotiation, and text message. The number of messages used for M2M authentication is minimised by using 6 messages between the server and the devices. The proposed protocol is safe and secure against various attacks in simulations based on automated verification of protocols and applications for Internet security.

The authors of [33] demonstrated that, with a suitable training mechanism, numerous M2M agents may successfully collaborate in a distributed manner, resulting in network performance that exceeds previous intelligence techniques in terms of convergence speed and achieving the EE and QoS criteria.

The encryption scheme with a dynamic key for M2M wireless communication described in [31], [34], [35] is based on exploiting the random and dynamic nature of the physical communication layer to develop low-cost encryption schemes. The authors consider the study of the dynamic key generation process. This is accomplished by combining a previously shared secret key extracted from a physical communication channel file with parameters shared by two M2M devices. Based on complex calculations, this scheme ensures a high level of security for M2M communications. It can eventually cause minor delays in the shared network of connected devices. A lighter method is used in this study. It aims to identify devices fairly quickly using simple algorithms that contribute to the creation of security for M2M communications.

5. Conclusion

The article discusses security methods for quickly resolving data processing issues by using the SoC's main machine to identify and authenticate the devices on 19 machines. The results suggest that machines can be vulnerable to data leaks and malware attacks when they are offline and processing different processes. This applies to both individual machines and the system as a whole. AnyLogic software was used to simulate the operation of 19 machines, 7 of which were subjected to unwanted data leakage processes and malware attacks.

The duration of data leakage with malware attacks for 4 machines was 70 s. The duration for 10 machines was 150 s with 3 attacks. Machine 15 had the longest attack duration, lasting 190 s and involving 6 malware attacks, while machine 19 had the shortest attack duration, lasting 200 s and involving 7 malware attacks. The highest numbers indicated that attempting to hack a system increased the risk of damaging a device, potentially resulting in the entire system with connected devices failing.

The obtained results have practical value because they demonstrate how, over time, processes of object identification and classification are carried out to recognise data from intelligent sensors in an offline communication system. Moreover, the process of device and machine authentication is examined to avoid negative scenarios during the operation of machines via wired communication. The use of wireless technologies to study M2M security methods and parameters adds scientific value to the results. Thus, unauthorized attacks by intruders employing malware can be detected over time, and the consequences of data processing can be avoided through intelligent control.

The results show that this protocol-based approach to using identification and authentication algorithms improves cyber-physical system security while also providing real-time monitoring of offline system security. In the future, we plan to conduct research with the participation of more computers.

Abbreviations: AS – authentication server; CC – current cluster; Dos – denial of service; EDGE – enhanced data rates for GSM evolution; EDDC – efficient device type detection and classification; EL – energy level; eUICC – embedded universal integrated circuit card; GPRS – general packet Radio Service; GSM – group special mobile; GT – global trust-score; HSM – hardware security modules; IT – information technology; LTE – long term evolution; M2M – machine-to-machine; NC – number of neighbors; ND – node degree; QCI – QoS (quality of service) class identifier; RISC – reduced instruction set of computers; RSA – Rivest, Shamir and Adleman; RSSI – received signal strength indication; SCA – side-channel attacks; SPD – successful packet delivery; SoC – security operations centre; TS – trust score; UICC – embedded universal circuit card; Wi-Fi – wireless fidelity; WSN – wireless sensor network; 4G – 4th generation.

Acknowledgments

Not applicable.

References

[1] P.N. Railkar, P.N. Mahalle, and G.R. Shinde, "Scalable trust management model for machine to machine communication in the Internet of Things using fuzzy approach," Turk. J. Comput. Math. Educ. (TURCOMAT), vol.12, no.6, pp.2483–2495, 2021, doi: 10.17762/turcomat.v12i6.5691.

[2] Z. Zhou, Y. Guo, Y. He, X. Zhao, and W.M. Bazzi, "Access control and resource allocation for M2M communications in industrial automation," IEEE Trans. Ind. Informat., vol.15, no.5, pp.3093–3103, 2019, doi: 10.1109/TII.2019.2903100.

[3] K. Mikhaylov, A. Moiz, A. Pouttu, J.M.M. Rapún, and S.A. Gascon, "LoRa WAN for wind turbine monitoring: Prototype and practical deployment," 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Moscow, pp.1–6, IEEE, 2018, doi: 10.1109/ICUMT.2018.8631240.

[4] P. Thota and Y. Kim, "Implementation and comparison of M2M protocols for Internet of Things," 2016 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence and Applied Informatics/1st Intl Conf on Big Data, Cloud Computing, Data Science & Engineering (ACIT-CSII-BCD), Las Vegas, NV, pp.43–48, IEEE, 2016.

[5] M.W.D. Saravia, R. Salvador, C.M. Palencia, and A.E.P. Zepeda, "Monitoring system for solar thermal station with IoT and M2M," 2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII), Managua, Nicaragua, pp.1–6, IEEE, 2017, doi: 10.1109/CONCAPAN.2017.8278533.

[6] P. Huang, B. Copertaro, X. Zhang, J. Shen, I. Löfgren, M. Rönnelid, J. Fahlen, D. Andersson, and M. Svanfeldt, "A review of data centers as prosumers in district energy systems: Renewable energy integration and waste heat reuse for district heating," Appl. Energy, vol.258, Article 114109, 2020, doi: 10.1016/j.apenergy.2019.114109.

[7] A. Barki, A. Bouabdallah, S. Gharout and J. Traore, "M2M security: Challenges and solutions," IEEE Commun. Surv. Tutor., vol.18, no.2, pp.1241–1254, 2016, doi: 10.1109/COMST.2016.2515516.

[8] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Netw., vol.11, no.8, pp.2710–2723, 2013, doi: 10.1016/j.adhoc.2013.05.003.

[9] M. El-Hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)," 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, pp.1–3, IEEE, 2017, doi: 10.1109/CSNET.2017.8242006.

[10] H. Hui, C. Zhou, S. Xu, and F. Lin, "A novel secure data transmission scheme in industrial Internet of Things," China Commun., vol.17, no.1, pp.73–88, 2020, doi: 10.23919/JCC.2020.01.006.

[11] M.T. Lazarescu, "Wireless sensor networks for the Internet of

Things: Barriers and synergies," Components and Services for IoT Platforms, pp.155–186, Springer, Cham, 2017.

[12] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," Ad Hoc Netw., vol.20, pp.96–112, 2014.

[13] J. Ma, Y.B. Guo, J.F. Ma, X.M. Liu, and Q. Li, "Multi-user access control scheme based on resources hierarchies for perceptual layer of IoT," Acta Electronica Sinica, vol.42, no.1, pp.28–35, 2014.

[14] O. Salman, S. Abdallah, I.H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, pp.1109–1111, IEEE, 2016, doi: 10.1109/ISCC.2016.7543884.

[15] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," Proc. 12th International Conference on World Wide Web, pp.640–651, Association for Computing Machinery, New York, NY, 2003.

[16] H. Isah and F. Zulkernine, "A scalable and robust framework for data stream ingestion," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, pp.2900–2905, IEEE, 2018, doi: 10.48550/arXiv.1812.04197.

[17] A.A. Corici, M. Corici, E. Troudt, B. Riemer, and T. Magedanz, "Framework for trustful handover of M2M devices between security domains," 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, pp.102–109, IEEE, 2020, doi: 10.1109/ICIN48450.2020.9059457.

[18] I. Bedhief, M. Kassar, and T. Aguili, "From evaluating to enabling SDN for the Internet of Things," 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, pp.1–8, IEEE, 2018, doi: 10.1109/AICCSA.2018.8612841.

[19] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain-based trust communities for decentralized M2M application services," International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp.62–73, Springer, Cham, 2018.

[20] F. Bao and I.R. Chen, "Dynamic trust management for Internet of Things applications," Proc. 2012 International Workshop on Self-aware Internet of Things, pp.1–6, Association for Computing Machinery, New York, NY, 2012, doi: 10.1145/2378023.2378025.

[21] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC), Sydney, NSW, Australia, pp.18–23, IEEE, 2012, doi: 10.1109/PIMRC.2012.6362662.

[22] T. Kaur and D. Kumar, "Computational intelligence-based energy efficient routing protocols with QoS assurance for wireless sensor networks: A survey," Int. J. Wirel. Mob. Comput., vol.16, no.2, pp.172–193, 2019.

[23] M.P. Lokhande, D.D. Patil, L.V. Patil, and M. Shabaz, "Machine-to-machine communication for device identification and classification in secure telerobotics surgery," Secur. Commun. Netw., vol.2021, Article 5287514, pp.1–16, 2021, doi: 10.1155/2021/5287514.

[24] A. Cubero-Fernandez, F.J. Rodriguez-Lozano, R. Villatoro, J. Olivares, and J.M. Palomares, "Efficient pavement crack detection and classification," J. Image Video Proc., vol.2017, no.1, pp.1–11, 2017, doi: 10.1186/s13640-017-0187-0.

[25] J.N. T.U. K. Kakinada and A. Pradesh, "Implementation of a group-based verification mechanism for secure M2M communications," J. Univ. Shanghai Sci. Technol., vol.22, no.12, pp.78–92, 2020.

[26] M.P. Lokhande and D.D. Patil, "Network performance measurement through machine to machine communication in tele-robotics system," Preliminary Commun., vol.15, no.1, pp.98–104, 2021, doi: 10.31803/tg-20210205092413.

[27] A. Esfahani, G. Mantas, R. Matischek, F.B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M.G. Tauber, C. Schmittner, and J. Bastos, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," IEEE Internet Things J., vol.6, no.1, pp.288–296, 2017, doi: 10.1109/JIOT.2017.2737630.

[28] M.M. Samy, W.R. Anis, A.A. Abdel-Hafez, and H.D. Eldemerdash, "An optimized protocol of M2M authentication for Internet of Things (IoT)," Int. J. Comput. Netw. Inf. Secur., vol.13, no.2, pp.29–38, 2021, doi: 10.5815/ijcnis.2021.02.03.

[29] W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) Winbond TrustME$^{\text{TM}}$ Secure Element Security Target Lite. Winbond, 2017. [Online]. Available at: https://www.commoncriteriaportal.org/files/epfiles/W76Sxx_SecurityTarget_Lite_A.pdf

[30] K.M. Renuka, S. Kumari, D. Zhao, and L. Li, "Design of a secure password-based authentication scheme for M2M networks in IoT enabled cyber-physical systems," IEEE Access, vol.7, pp.51014–51027, 2019, doi: 10.1109/ACCESS.2019.2908499.

[31] H. Noura, R, Melki, A. Chehab, M.M. Mansour, and S. Martin, "Efficient and secure physical encryption scheme for low-power wireless M2M devices," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, pp.1267–1272, IEEE, 2018, doi: 10.1109/IWCMC.2018.8450330.

[32] U. Singh, A. Dua, N. Kumar, S. Tanwar, R. Iqbal, M. Hijii, S. Amin, and R. Sharma, "Scalable priority-based resource allocation scheme for M2M communication in LTE/LTE-A network," Comput. Electr. Eng., vol.103, Art. no.108321, 2022, doi: 10.1016/j.compeleceng.2022.108321

[33] X. Li, X. Wei, S. Chen, and L. Sun, "Multi-agent deep reinforcement learning based resource management in SWIPT enabled cellular networks with H2H/M2M co-existence," Ad Hoc Networks, vol.149, Art. no.103256, 2023, doi: 10.1016/j.adhoc.2023.103256.

[34] I. Sagynganova, A. Kalinin, K. Smagulova, D. Lissitsyn, and D. Abulkhairov, "SMART system for the implementation of rational heat-supply regimes," Polityka Energetyczna, vol.25, no.2, pp.137–146, 2022, doi: 10.33223/epj/149889.

[35] A. Kintonova, A. Sabitov, I. Povkhan, D. Khaimulina, and G. Gabdreshov, "Organization of online learning using the intelligent metasystem of open semantic technology for intelligent systems," East.-Eur. J. Enterp. Technol., vol.121, no.2, pp.29–40, 2023.

Ya Zhong holds Bachelor's degree. Ya Zhong is currently an Associate Professor of the Department of Information Engineering at Tongren Polytechnic College, Tongren. Research interests: machine-to-machine communication; trust; wireless systems; offline operation; data transmission; Internet of Things; intelligent control.