An AODV Based Multifactor Authentication Scheme for Wireless Sensor Network

[1]Jane Zhen Zhen Yong, [2]Zi Jian Chai, [3]Kah Hao Chin, [4]Christopher Chin Fung Chee, [5]Daniel Kung Min Soh, [6]Jing Yong Kwong and [7]Wei Yin Ooi
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
email: [1]yongjane013@gmail.com, [2]chai19971@live.com, [3]chinckh97@gmail.com, [4*]christophercheezhenfung@gmail.com, [5]danielsoh97@gmail.com, [6]jykwong97@gmail.com

Date received: 24 August 2021
Date accepted: 22 October 2021
Date published: 8 November 2021

Abstract – *Wireless Sensor Network (WSN) is a type of wireless network that is fast getting a lot of attention in scientific and industrial applications, and it is a network of decentralized autonomous standalone sensor devices. However, WSN is easily prone to malicious attacks as anyone can access the server through the node without a proper security authentication. In this paper, we proposed a secure AODV based multi-factor authentication scheme for WSN to mitigate physical attack, offline guessing attack and replay attack. Our proposed scheme is preferred to keep the scheme lightweight while providing enough security that requires smart card, user identity, password, and OTP. Our proposed scheme has relatively lower computational cost with a total of 10Th than the other compared schemes except for Adil et al.'s scheme. However, we have around 8288 bits of authentication overhead due to the nature of packet and the addition of factors. Hence, our scheme is outperformed from computational cost perspective, but the scheme is slightly higher on authentication overhead perspective. In the future, multiple device authentication, implementation of biometric feature can be added to improve the scheme.*

Keywords: High authentication overhead, lightweight, lower computational cost, malicious attack, multi-factor authentication.

1 Introduction

Industry 4.0, also known as the Fourth Industrial Revolution had changed the way businesses operate. The automation of industrial processes requires a secure network connection with the devices to allow them to extract and control data in the real time (Pena-Cabrera et al., 2019). Manufacturing industry is the main industry in applying this revolution as it contributed the most income to Malaysia's economy. Then, as the rapid development on technology in IR4.0 transition, the old technique in manufacturing industry is gradually moving into wireless sensor network (WSN) (Ahmad et al., 2019). WSN is a type of wireless network that is fast getting a lot of attention in scientific and industrial applications, and it is a network of decentralized autonomous standalone sensor devices (Zhou et al., 2019). For example, the sensor devices can be used to monitor physical or environmental factors such as temperature, pressure, humidity, and pollution levels while transmit the information to a base station (Durugkar & Poonia, 2017; Ezhilazhahi & Bhuvaneswari, 2017; Nooriman et al., 2018; Guanochanga et al., 2018; Gope et al., 2019; Ferentinos et al., 2017; Chen et al., 2019). Due to the wireless characteristics of WSN, it is always the target of malicious attacks (Li et al., 2018).

As WSN deployed in an open environment, it is easily subject to physical attacks as anyone can access the server through the node without proper security authentication. Instead of that, current WSNs are struggled to mitigate those attacks due to their constrained nature (Adil et al., 2020). It is difficult for the current existing scheme to minimize the computational cost and authentication overhead. At the same time, maximize their security levels to protect the networks from attacks as much as possible. For example, MAC-AODV based mutual authentication

scheme proposed by Adil et al. (2020) can address the confidentiality and authenticity issues while keeping the scheme computationally efficient. However, the uniqueness of this scheme is using the 48-bits MAC addressing scheme during the registration phase and later used as the unique identifier for the sensor node had led to high communication overhead, 6144 bits (Adil et al., 2020). Another scheme is the two-factor authenticated key agreement scheme proposed by Shin and Kwon (2018) provides strong anonymity, which can withstand attacks like session-specific temporary information attack, physical attack, offline password guessing attack etc. The drawback of this scheme is it requires more computational steps to ensure strong anonymity (Shin & Kwon, 2018). Furthermore, an efficient and provably secure anonymous user authentication scheme proposed by Xu et al. (2020) used Rabin cryptosystem and chaotic maps to establish the minimal cost of the secure session key. It used the hardness of large number prime factorization and Chebyshev chaotic Diffie-Hellman problem to increase its security (Xu et al., 2020). The disadvantage of this scheme is it incurred a high computation overhead to provide more security attributes.

Hence, in this paper, we proposed a secure AODV based multi-factor authentication scheme for WSN while balancing the overall communication and computation overhead. The proposed scheme should mitigate attacks like physical attacks mitigation in Shin and Kwon's scheme, impersonation attacks mitigation in Adil et al.'s scheme and replay attacks mitigation in Xu et al.'s scheme.

A balanced and secure multifactor authentication scheme is preferred to keep the scheme lightweight while providing enough security that requires smart card, user identity, password, and OTP. With the usage of smartcard, user identity and password, the scheme can secure from the physical attack such as sensing device stolen issue. With the addition of OTP, the performance is expected to be improved rather than the previous scheme proposed by Adil et al. as it can prevent the attackers from obtaining secret codes that is send through the user's phone. Also, it can be invalid in minutes and prevent the attackers from reusing them.

Our proposed scheme has relatively lower computational cost with a total of $10T_h$ than the other proposed scheme by Shin & Kwon that requires more computational steps to ensure strong anonymity and Xu et al. that use Rabin cryptosystem and chaotic maps to increase the security of the proposed scheme. However, our proposed scheme has higher computational cost which is greater than the original scheme by Adil et al. due to OTP and smart card has been added to enhance the security level. Besides, we have around 8288 bits of authentication overhead due to the nature of packet and the addition of factors like user identity, password, and OTP. Hence, our scheme is outperformed from computational cost perspectives if compared with Shin and Kwon's scheme and Xu et al.'s scheme.

The main contributions of this research work are described as below:

1) A smartcard access device authentication algorithm that mitigates physical attack.
2) The proposed approach uses masked identity and password for authentication purpose.
3) Base station generates One-Time-Password (OTP) and nonce k_i to mitigate replay attack.

In general, Industry 4.0 will expose maximum personal information the world has ever seen (Onik et al., 2019). Hence, a new, and secure authentication schemes have always been researched to deal with the data privacy and security issues. In the future, our proposed scheme can include additional biometric factor, use the same smartcard to access multiple devices and lastly is the multiple device authentication algorithm enhancement.

2 Related works

This section summarizes different types of authentication schemes for wireless sensor networks (WSN). Over the years, WSN has become an epidemic technology that involved in various applications such as agriculture, health care, surveillance systems and incident management (Moghadam et al., 2020). Many schemes have been proposed to enhance the security level of the WSN.

In 2018, Shin and Kwon proposed a two-factor mutual authentication scheme that using the cryptographic algorithm such as hashed function, masked identity, password and XOR operation to mitigate several attacks (Shin & Kwon, 2018). However, this scheme has a higher computational cost and authentication overhead.

One protocol proposed by Yu et al. in 2020 has mutual authentication, anonymity, and untrace ability characteristics which helps in securing the networks from replay attack, smart card theft attack and impersonation attack (Yu et al., 2020).

Another protocol is anonymous key-agreement protocol suggested by Ahmed et al. (Ahmed et al., 2020). The protocol used a multifactor authentication compact key agreement approach to overcome the vehicle to grid networks' privacy and security problems to permit its wide interconnection to smart grids in 2020. The proposed approach preserves the security of communication and allows user and trusted side to verify each other's validity. To strengthen data security, the compact encryption algorithms such as exclusive-OR and hash are applied. This protocol provides protection from attacks like replay attacks, smart card stolen attacks, man-in-the-middle attacks, and so on (Ahmed et al., 2020).

In the same year, Umar et al. had proposed a mutual authentication and data encoding scheme based on signal propagation characteristics for distinguishing between legitimate and attacker devices, and enhanced butterfly algorithm. This scheme has a well performance in security as it can withstand several attacks such as man-in-the-middle attack, passive and active eavesdropping attacks, impersonation attack, stolen verifier attack, and data replay attack. By using this scheme, opponents have no access to the initial key so they will experience failure in the trial of message decryption (Umar et al., 2020).

The next scheme is designed for patient monitoring using wireless medical sensor networks. It is proposed by Xu et al., which is secured against potential attacks such as off-line guessing attack, replay attack, etc. It provides an efficient and secure biometric authentication using Rabin cryptosystem and chaotic maps to establish a secure session at a minimum cost. However, it is slightly inferior in communication overhead due to the Rabin cryptosystem (Xu et al., 2020).

To ensure a secure, robust, and lightweight authentication, Masud et al. proposed a Mutual Authentication and Secret Key (MASK) protocol for the healthcare system. This proposed scheme applied bitwise XOR operations, one-way hash function, physical unclonable functions and nonce to mitigate physical attacks, man-in-the-middle attacks and impersonations attacks (Masud et al., 2021).

Moreover, Adil et al. solve the confidentiality and authenticity issues using the 48-bits MAC addressing scheme (Adil et al., 2020). Besides, the scheme also implemented with AODV protocol. According to Desai et al. (2017), AODV uses one entry per destination and traditional routing tables while finding the new routes when the route that is available in the routing table fails (Desai et al., 2017). To prevent loops of routing, AODV uses sequence numbers so that the most recent route can be identified by AODV. It has a low connection setup delay, and its paths are only available once requests (Rana & Kumar, 2019). Apart from AODV protocol, Adil et al. also used elliptic curve deffi-hellman problem (ECDDHP) and elliptic curve integrated encryption scheme (ECIES) to encrypt the data packet (Adil et al., 2020). According to Phimphinith et al., the ECDDHP can ensure that the attackers cannot reach from one point to another point given two points because they do not have ability to compute the multiplicand (Phimphinith et al., 2019). By applying this concept in Adil et al.'s scheme, it is securing the network from the impersonation attack. With ECIES, it further secures the data packet from the attack because it uses key agreement function, key derivation function, public-key cryptography algorithm and lastly hash function (Choi et al., 2020). However, the scheme is still vulnerable to attacks like physical attacks and replay attacks (Adil et al., 2020). Hence, the proposed solution will solve the issues that arise from the Adil et al.'s scheme.

3 Proposed solution

Modification and enhancement are made on the MAC-AODV based mutual authentication scheme to resolve the aforementioned issue. The proposed scheme consists of two phases, the registration phase, and the authentication phase. It is a multifactor authentication scheme that use smartcard, identity, password, and One-Time-Password (OTP) during the authentication phase. The scheme also eliminates the usage of the mac address to reduce the redundancy. Overall, the scheme might have a slightly higher authentication overhead but lower computational cost perspective than the other compared schemes except for Adil et al.'s scheme. In addition, the physical attack and replay attack problems can be fixed using this scheme. Attack mitigation details will be discussed in the security analysis section.

There is a several assumptions for the proposed scheme which is listed as below:

i. First time registration time, T_P from requesting, T_{REQ} to responding time, T_{RES} is recorded and used as timestamp validation during the authentication.
ii. The network delay and packet loss are negligible in the test environment.
iii. One sensing device can only be registered with one smartcard.

Besides, the important notations to describe the proposed scheme are listed in Table 1.

Table 1: Notation for proposed scheme

Symbol	Definition
SC_i	Smart Card
ID_i	User Identity
PW_i	User Password
PN_i	User Phone Number
MID_i	Masked Identity
MPW_i	Masked Password
MPN_i	Masked Phone Number
Pkt	Packet
B_c	Bash Value
src	Source Address
ds	Destination Address
AODV	Ad-hoc On-demand Distance Vector
ECIES	Elliptic Curve integrated Encryption Scheme
ECDDHP	Elliptic Curve Deffi-hellman Problem
H	Hash
E_t	Encrypt
a_i, b_i	Random Static Number
r_i , k_i	Random Nonce

Below is the procedure on how the registration and authentication process works.

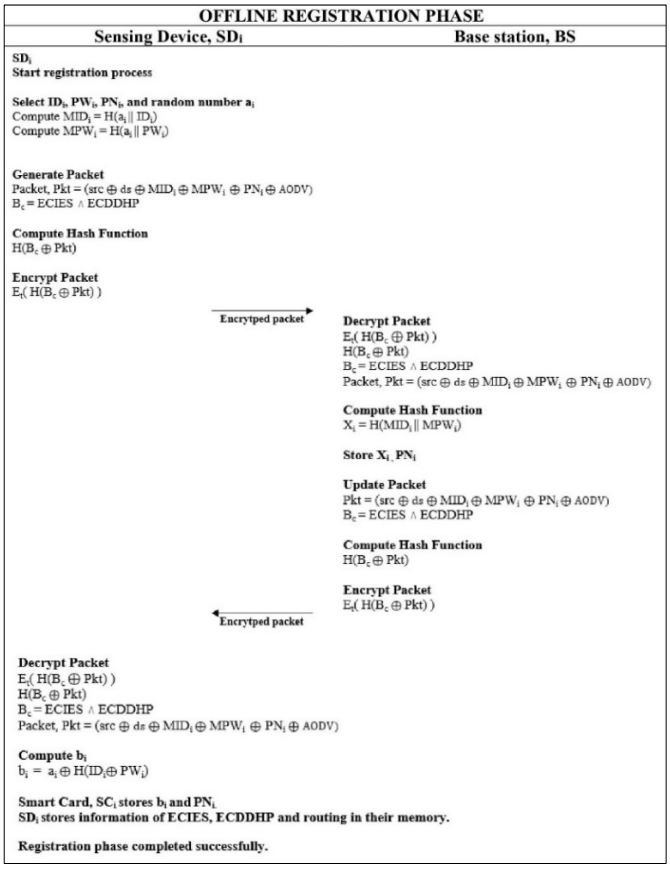

Figure 1: Offline registration phase.

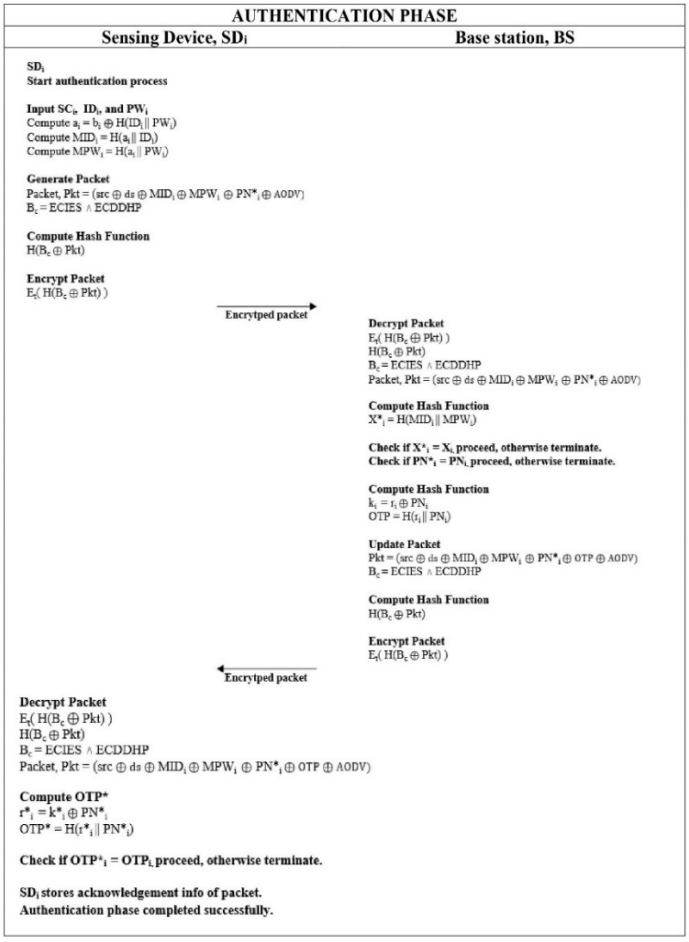

Figure 2: Authentication phase.

3.1 Device and Smart Card Registration Phase

This registration phase is carried out in offline mode. A new smartcard is required to register with the base station when there is a new sensing device. Below is a detailed explanation of the registration steps.

(1) User inserts smartcard SC_i to the sensing device SD_i and inputs identity ID_i, password PW_i and phone number PN_i. SD_i generates a random number a_i and compute $\mathbf{MID_i = H(a_i \,||\, ID_i)}$ and $\mathbf{MPW_i = H(a_i \,||\, PW_i)}$.

(2) SD_i starts to generate request packet. The packet contains information like source address, destination address, masked identity, masked password, phone number with Ad-hoc On-demand Distance Vector AODV protocol. The packet also will be encrypted together with the ECDDHP and ECIES.

(3) SD_i starts to hash the packet after the request packet is ready ($\mathbf{H(B_C \oplus Pkt)}$).

(4) SD_i encrypts the packets using an asymmetric cryptography algorithm and sends to base station BS through a secure channel.

(5) After receiving the SD_i' s request packet, BS decrypts the packet to obtain the content.

(6) After the decryption process, BS computes $\mathbf{X_i = H(MID_i \,||\, MPW_i)}$ and stores X_i, PN_i and SD_i's request timeframe, T_{REQ} in BS.

(7) BS generates the response packet with the information required, such as the SD_i's request timeframe and the BS's response timeframe. This information is important for timestamp validation purpose during the authentication phase.

(8) BS starts to hash the packet after the response packet is ready ($\mathbf{H(B_C \oplus Pkt)}$).

(9) BS encrypts the packets using an asymmetric cryptography algorithm and sends to SD_i through a secure channel.

(10) After receiving the BS's response packet, SD_i decrypts the packet to obtain the content.

(11) After the decryption process, SD_i computes $\mathbf{b_i = a_i \oplus H(ID_i \oplus PW_i)}$ and stores b_i and PN_i in SC_i.

(12) Lastly, SD_i stores the information of ECIES, ECDDHP, routing and critical information like the BS's response timeframe T_{RES}.

3.2 Device and Smart Card Authentication Phase

This authentication phase is carried out in online mode after the SD_i is registered under the BS. Below is a detailed explanation of the authentication steps.

(1) The user inserts SC_i to the SD_i and inputs ID_i and PW_i and SD_i generates $\mathbf{a_i = b_i \oplus H(ID_i||PW_i)}$ using b_i stored in SC_i. a_i is then used to compute $\mathbf{MID_i = H(a_i || ID_i)}$ and $\mathbf{MPW_i = H(a_i || PW_i)}$.
(2) SD_i starts to generate request packet. The packet contains information like source address, destination address, masked identity, masked password, phone number with Ad-hoc On-demand Distance Vector AODV protocol. The packet also will be encrypted together with the ECDDHP and ECIES.
(3) SD_i starts to hash the packet after the request packet is ready ($\mathbf{H(B_C \oplus Pkt)}$).
(4) SD_i encrypts the packet using an asymmetric cryptography algorithm and sends to base station BS through a secure channel.
(5) After receiving the SD_i' s request packet, BS decrypts the packet to obtain the content.
(6) After the decryption process, BS will first check the current timestamp with the requested packet's timestamp. If the requested packet takes a longer time than the expected time T_{REQ}, BS will discard that packet. If the requested packet is reached to the BS within the expected time, then BS will proceed to the next step.
(7) BS checks PN^*_i with PN_i stored in the BS. If it is matched, proceed to the next step. Else, BS will discard the packet.
(8) BS computes $\mathbf{X^*_i = H(MID_i || MPW_i)}$. Then, BS will check X^*_i with X_i stored in the BS's memory. If it is matched, BS will accept the packet and proceed to the next step. Else, BS will discard the packet.
(9) BS generates a random nonce r_i, compute nonce $\mathbf{k_i = r_i \oplus PN_i}$ and send k_i to the registered PN_i. BS is then compute OTP using hash operation $\mathbf{H(r_i||PN_i)}$.
(10) BS generates the response packet with additional information of OTP.
(11) BS starts to hash the packet after the response packet is ready ($\mathbf{H(B_C \oplus Pkt)}$).
(12) BS encrypts the packet using an asymmetric cryptography algorithm and sends to SD_i through a secure channel.
(13) After receiving the BS's response packet, SD_i decrypts the packet to obtain the content.
(14) After the decryption process, SD_i will first check the response timestamp with the current timestamp. If the response packet takes longer time than the expected time T_{RES}, SD_i will discard that packet. If the response packet is reached to the SD_i within the expected time, then SD_i will proceed to the next step.
(15) User needs to input k^*_i value to the SD_i in which k^*_i is sent to the phone number PN^*_i. SD_i will compute r^*_i using k^*_i from the input and PN_i stored in the SC_i ($\mathbf{r^*_i = k^*_i \oplus PN_i}$).
(16) SD_i uses the r^*_i computed earlier to compute OTP* ($\mathbf{OTP^* = H(r^*_i || PN_i)}$). Then, SD_i will check OTP* with OTP received from the packet. If it is matched, SD_i accepts the packet and stores the acknowledgement info. Else, discard the packet.

4 Security Analysis

In this section, the proposed scheme resilience against well-known attacks is discussed in detail. As mentioned in previous section, the scheme is proposed based on the modification of Adil et al.'s scheme. Previously, Adil et al.'s scheme can secure against well-known attacks like impersonation attack and eavesdropping attack (Adil et al., 2020). However, it is vulnerable to physical attack and replay attack because it only involved single factor mutual authentication. Hence, the proposed scheme will be able to mitigate the attacks as discussed in the Adil et al.'s scheme; the physical attack, replay attack and off-line guessing attack that we discovered.

4.1 Resistance to Physical Attack

Assume that an adversary has physically capture the device. The adversary prepares to send the login information request that use to connect the communication process with the base station. However, the adversary with the device is unable to reveal the identity of device. This is because the adversary unable to obtain b_i where b_i is stored inside the smartcard. Hence, without the smart card, adversary is unable to compute correct a_i to further compute the hash function for identity and password masking, $a_i = b_i \oplus H(ID_i||PW_i)$. Thus, the base station cannot authenticate the device because it will produce different X^*_i value due to incorrect masked identity and password. Therefore, the scheme is secure against physical attack.

4.2 Resistance to Off-line Guessing Attack

Suppose that adversary compromise the smart card and device and attempts to guess the identity (ID) and password (PW). If adversary successfully capture the ID and PW, he needs to input the correct k_i for OTP

validation. When base station (BS) receives the login information request, it generates the k_i and send to user's phone if everything is correct. When the k_i entered is wrong, the BS regards that it come from an attacker and terminate the connection. Hence, the scheme is secure resistance to off-line guessing attack, even the smart card and device are compromised, and ID and PW are successfully capture.

4.3 Resistance to Replay Attack

In the base station, nonce k_i and r_i are intended to prevent replay attack. The nonce r_i is involved in the hash value of OTP. In case of getting the nonce r_i, the adversary is required to compromise the user's phone to get the k_i, since the $r_i$is generated by k_i within certain time. Besides that, the timestamps are used to verify the freshness of request and response message. The timestamp can be checked through $|\text{current} - \text{request@response}| \leq \text{T}_{REQ}@\text{T}_{RES}$.Once the calculated timestamps exceed the recorded timestamps, they are expired, the communication process will be terminated. The OTP validation and timestamp validation contribute to the double protection layer to the replay attack. Hence, it proved that the scheme is secure against the replay attack because it is difficult for the adversary to pass both validations at the same time.

5 Complexity Analysis

In this section, the estimated authentication overhead and computation cost are compared with other schemes. Based on the result, we noticed that the proposed scheme has slightly higher authentication overhead as it solves the problems arise from previous scheme but lower computation cost than the compared original scheme except for Adil et al.'s scheme. The overhead due to the additional factors is acceptable in this case. The details are shown in sub-section below.

5.1 Authentication Overhead

Authentication overhead can greatly affect effectiveness of the scheme especially in a constraint area network. Hence, we have assumed that the data packets transferred contain only important and critical information for authentication purpose during the registration and authentication phase. Moreover, we also assumed that the authentication overhead is always constant in an ideal scenario. The result is shown in Table 2 below.

Table 2: Comparison of the authentication overhead

Scheme	Total authentication overhead (in bits)
Shin & Kwon (Shin & Kwon, 2018)	4160
Adil et al. (Adil et al., 2020)	6144
Xu et al. (Xu et al., 2020)	2304
Proposed	8288

Based on the analysis, we estimated that the proposed scheme will have 8288 bits of authentication overhead. We estimated this value based on Adil et al.'s scheme and Shin & Kwon's scheme. In Adil et al.'s scheme, there is total of six messages transferred with 6144 bits (Adil et al., 2020). Based on this value, we assumed that each message would have 1024 bits, but since the 48-bits MAC address is removed from our proposed scheme, then each message in our proposed scheme will have 976 bits. In Shin & Kwon's scheme, they assumed that the lengths of the identity and password are each 128 bits (Shin & Kwon, 2018). By applying the same assumption as stated by Shin & Kwon, the proposed scheme will have extra 384 bits per message due to the addition of masked identity, masked password, and phone number for the first five message and the last message will have extra 512 bits due to the addition of OTP with the data explained earlier. The calculation is as shown below.
Adil et al.'s scheme (Adil et al., 2020): $1024\ bits\ *\ 6\ messages$ = 6144 bits
Shin & Kwon's scheme (Shin & Kwon, 2018): Length of identity/ password/ hash function output = 128 bits
Our proposed scheme:
First five messages = (1024 - 48) + (128 x 3)
= 1360 bits per message
Last message = (1024 - 48) + (128 x 4)
= 1488 bits per message
Total = (1360 x 5) + 1488 = 8288 bits

In this sub-section, the total computation cost of the scheme is compared with other schemes. One of the assumptions when we estimated the computation cost is we assumed that the nonce and XOR calculation cost are

neglectable. Thus, we only calculated the estimated cost based on the number of hash function performed. This led to another assumption which is the computational time to compute is constant in an ideal scenario. The result is shown in Table 3 below.

Table 3: Comparison of the computational cost

Scheme	Total computation cost (T_h)
Shin & Kwon (Shin & Kwon, 2018)	53
Adil et al. (Adil et al., 2020)	4
Xu et al. (Xu et al., 2020)	15
Proposed	10

Based on our discussion and analysis, we estimated that the proposed scheme will have $10T_h$ for authentication phase. The cost is greater than the original scheme proposed by Adil et al. because we added few factors such as identity, password and OTP to enhance its security level. Comparing to other scheme, the cost is minimal as those schemes are complicated in computation.

6 Conclusion

The "MAC-AODV based mutual authentication" scheme proposed by Adil et al. focuses on mitigation of impersonation attack. However, the previous scheme is vulnerable to physical attack and replay attack (Adil et al., 2020). Hence, we designed a solution called An AODV Based Multifactor Authentication Scheme to overcome the security threats. Its multi-factor authentication process requires smartcard, user id, password, and OTP. By using these factors, the scheme is secured from physical attack if the sensing device is compromised. The performance is expected to be improved due to addition of OTP become invalid in minutes, thus this will prevent attackers from obtaining secret codes and reusing them. By making a full comparison of the proposed and similar schemes to assure the validation of efficiency and security, the proposed scheme is obviously more effective against to physical attack and replay attack. Moreover, our protocol scheme is more efficient in terms of communication and computation costs according to the results of the performance analysis. Hashing function is encouraged to be implemented in the proposed scheme due to its low authentication overhead and computation cost. Our proposed scheme achieved a result of 10 T_h in the computation phase. Additionally, the authentication overhead in our proposed scheme would be 8228 bits due to the addition of extra factors. In the future work, more than one device accesses by using the same card can be made available so that it is more applicable to actual environment while ensuring efficient and secure authentication. The proposed scheme also can be improved by enhancing the user's biometrics thumb impression used for the local authentication of password between the sensing device and base station using the Physically Unclonable Function (PUF). PUF generally is used for secure authentication and secure communication in between both parties as it does not require any classical cryptographical assets, hence it can easily overcome the cost of sensing devices (Gope et al., 2019). Moreover, multiple devices authenticate each other is needed to incorporate in the proposed scheme because direct communication in the current scheme is not always ideal.

References

Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV Based Mutual Authentication Scheme for Constraint Oriented Networks. IEEE Access, vol. 8, pp. 44459-44469.

Ahmad, M. I., Yusof, Y., Adam, A., & Daud, M. (2019). Machine Process Condition Monitoring with 3MP. 2019 4th International Conference on Electromechanical Control Technology and Transportation (ICECTT).

Ahmed, S., Kumari, S., Saleem, M., Agarwal, K., Mahmood, K., & Yang, M. (2020). Anonymous Key-Agreement Protocol for V2G Environment Within Social Internet of Vehicles. IEEE Access, vol. 8, pp. 119829-119839.

Chen, M., Lee, T., & Pan, J. (2019). An Enhanced Lightweight Dynamic Pseudonym Identity Based Authentication and Key Agreement Scheme Using Wireless Sensor Networks for Agriculture Monitoring. Sensors, vol. 19, no. 5, p. 1146.

Choi, J., Kim, D., Choe, J., & Shin, K. (2020). Hardware Implementation of ECIES Protocol on Security SoC. 2020 International Conference on Electronics, Information and Communication (ICEIC).

Desai, R., Patil, B., & Sharma, D. (2017). Routing Protocols for Mobile Ad Hoc Network - A Survey and Analysis. Indonesian Journal of Electrical Engineering and Computer Science, vol. 7, no. 3, pp. 795-801.

Durugkar, S., & Poonia, R. (2017). Optimum utilization of natural resources for home garden using wireless sensor networks. Journal of Information and Optimization Sciences, vol. 38, no.6, pp. 1077-1085.

Ezhilazhahi, A., & Bhuvaneswari, P. (2017). IoT enabled plant soil moisture monitoring using wireless sensor networks. 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS).

Ferentinos, K., Katsoulas, N., Tzounis, A., Bartzanas, T., & Kittas, C. (2017). Wireless sensor networks for greenhouse climate and plant condition assessment. Biosystems Engineering, vol. 153, pp. 70-81.

Gope, P., Das, A., Kumar, N., & Cheng, Y. (2019). Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, vol. 15, no. 9, pp. 4957-4968.

Guanochanga, B., Cachipuendo, R., Fuertes, W., Salvador, S., Benitez, D. S., Toukeridis, T., . . . Meneses, F. (2018). Real-Time Air Pollution Monitoring Systems Using Wireless Sensor Networks Connected in a Cloud-Computing, Wrapped up Web Services. Proceddings of the Future Technologies Conference (FTC), pp. 171-184.

Li, X., Niu, J., Bhuiyan, M., Wu, F., Karuppiah, M., & Kumari, S. (2018). A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3599-3609.

Masud, M., Gaba, G. S., Alqahtani, S., Muhammad, G., Gupta, B. B., Kumar, P., & Ghoneim, A. (2021). A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. IEEE Internet of Things Journal, pp. 1-1.

Moghadam, M., Nikooghadam, M., Jabban, M., Alishahi, M., Mortazavi, L., & Mohajerzadeh, A. (2020). An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network. IEEE Access, vol. 8, pp. 73182-73192.

Nooriman, W., Abdullah, A., Rahim, N., & Kamarudin, K. (2018). Development of wireless sensor network for Harumanis Mango orchard's temperature, humidity and soil moisture monitoring. 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE).

Onik, M., Kim, C., & Yang, J. (2019). Personal Data Privacy Challenges of the Fourth Industrial Revolution. 2019 21st International Conference on Advanced Communication Technology (ICACT).

Pena-Cabrera, M., Lomas, V., & Lefranc, G. (2019). Fourth industrial revolution and its impact on society. 2019 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON).

Phimphinith, A., Anping, X., Zhu, Q., Jiang, Y., & Shen, Y. (2019). An Enhanced Mutual Authentication Scheme Based on ECDH for IoT Devices Using ESP8266. 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN).

Rana, R., & Kumar, R. (2019). Performance Analysis of AODV in Presence of Malicous Node. Acta Electonica Malaysia, vol. 3, no. 1, pp. 1-5.

Shin, S., & Kwon, T. (2018). Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks. IEEE Access, vol. 6, pp. 11229-11241.

Umar, M., Wu, Z., & Liao, X. (2020). Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics. IEEE Access, vol. 8, pp. 66411-66422.

Xu, G., Wang, F., Zhang, M., & Peng, J. (2020). Efficient and Provably Secure Anonymous User Authentication Scheme for Patient Monitoring Using Wireless Medical Sensor Networks. IEEE Access, vol. 8, pp. 47282-47294.

Yu, S., Lee, J., Park, K., Das, A., & Park, Y. (2020). IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment. IEEE Access, vol. 8, pp. 167875-167886.

Zhou, B., Li, S., Wang, W., Wang, J., Cheng, Y., & Wu, J. (2019). An Efficient Authentication Scheme Based on Deployment Knowledge Against Mobile Sink Replication Attack in UWSNs. IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9738-9747.