Chain Identity Attestation (CIA) Method for Preventing Node Cloning Attack in Wireless Sensor Network

Norhaflyza Marbukhari, Yusnani Mohd Yussoff, Syed Farid Bin Syed Adnan, Mohd Anuar Mat Isa and Nazhatul Hafizah Kamarudin
InSTIL Research Initiative Groups, Computer Engineering Department,
University Teknologi MARA (UiTM) Shah Alam, Selangor, Malaysia.
eijafly@gmail.com

***Abstract*—This paper presents a new technique in preventing node cloning attack. The significant contribution of this method or technique is in preventing node impersonation attack in Wireless Sensor Network (WSN). The new method named as Chain Identity Attestation Method (CIA) was developed on the basis of Diffie-Hellman hard problem algorithm. The exclusivity of CIA method is in the generation of node identity. In this method, the node identity is in each session. In other words, node identity is no longer fixed to a certain value. Perfect forward secrecy attack model is used to prove the security of this CIA method.**

***Index Terms*—Node Identity; Node Impersonation; Trusted Sensor Node; Wireless Sensor Network.**

I. INTRODUCTION

A WSNs system incorporates a gateway that provides wireless connectivity back to the wired environment and distributed nodes. The nature of the sensor nodes that are located remotely and unattended has exposed itself to the node cloning attack. Node cloning attacks can be further classified into physical attack where the nodes are removed from their locations and being duplicated in the lab. The cloned nodes will then be placed at the original node locations to get access to the network. These cloned nodes will be programmed to report or to provide false messages to the base station. It will then result in invalid data and reaction. Another type of node cloning attack is node impersonation. If the base station or the communication network depends merely on the identity, the impersonated nodes will be able to join the network and will cause false or invalid data transmission to the network. This type of threat will also interfere with the trust management system in deciding trusted sensor nodes in the wireless sensor network.

This paper presents a new method in generating the identity for the sensor node to prevent node impersonation in the wireless sensor network. In this implementation, the identity of the sensor node will be different in each communication. The identity will be developed using Diffie-Hellman hard problem equation and in the form of chain identity. The aim of this method is to generate a chain of unique identity of the sensor node.

II. MOTIVATION

This work aims to mitigate node impersonation attack in the WSN environment or any embedded devices that demand unique identity. Consideration on the limitation of the sensor node or embedded devices such as limited power and processing capabilities has been taken into account throughout the designed process.

A. Objectives

The objective of this work is to develop a new technique in mitigating node impersonation attack. The idea is to have a chain of identity that uniquely identifies a specific sensor node. This technique will then be verified using Perfect Forward Secrecy attack model.

B. Target Application

The method developed is suitable for any embedded device that demands identity, such as applications involving e-health, e-transport, and many more. This method allows member in the network to authenticate with each other using different identity.

III. RELATED WORKS

This section discusses related work in the area of node cloning. It highlights the study on the node cloning followed by sequence of techniques in mitigating node cloning. The method used by Capkun et al. [5] is to check vulnerabilities in node positioning that ultimately aims to provide secure network. They found out that the distance estimation and bounding techniques are also very effective to secure the network from malicious attacker and dishonest node. This work identifies positions with capabilities of vulnerability. M. Ding [6] presents his works on fault sensor identification and fault-tolerant event boundary detection. However, current algorithms are sensitive to the settings of thresholds. Both works aforementioned utilized simulation technique. Researcher in Kyasanur [7] on the other hand, modify IEEE 802.11 MAC protocol that simplifies detection of such selfish host and also a correction scheme for this misbehaviour. The correction they proposed is effective in restricting the selfish nodes to a fair share.

On the other hand, K. Xing in [8] has implemented his study in real time. In this research, a base station is used to protect the network from the clone node. The base station will collect the information from all sensors in the network. This method results in high communication overhead especially when the base station requests information from

the sensor nodes in the network. However, the clone node can still send the data from the original node and thus the base station still fail to identify the cloned node. In [9], they proposed an elliptic curve discrete logarithm and bilinear pairing for their secure signature scheme. In their work, the secret key is associated with an identity and the signer just uses the current secret key with ID to sign the message, which is more practical.

Another work presented in [11] utilised trusted third party where each group will establish connection by communicating through a trusted third party. In this paper, a novel group key management scheme is proposed with perfect forward secrecy. The goal of this paper is to prevent any key exchange from being compromised among n-parties, who shares a common secret over an insecure network. Wu proposed an efficient smart card-oriented remote login authentication scheme. In [12] paper, they have drawn the attention to the weakness of Wu's system by demonstrating authentication request, replaying an eavesdropped message, and different attack schemes on deriving secret data from the eavesdropped messages. The analysis shows that our modified scheme can withstand all possible attacks while keeping its efficiency.

Then [13] proposed two novel node clone detection protocols with different trade-offs on network conditions and performance. The first one is based on a distributed hash table, which forms a Chord overlay network and provides the key-based routing, caching, and checking facilities for clone detection. Whilst the second one uses probabilistic directed technique to achieve efficient communication overhead for satisfactory detection probability. The DHT-based protocol provides high level security for all kinds of sensor networks by one deterministic witness, additional memory-efficiency, probabilistic witnesses, and the randomly directed exploration presents outstanding communication performance and minimal storage consumption for dense sensor networks. In [14] they proposed a secure dynamic ID-based remote user authentication scheme for the multi-server environment using smart cards and claimed that their scheme could protect against masquerade attacks, server spoofing attack, registration server spoofing attack and insider attack. They presented the cryptanalysis scheme that specified and analysed the proposed dynamic identity-based remote user authentication scheme for multi-server architecture using smart cards.

From the multitude of studies described above, there are numerous methods aim to prevent node cloning attack. Each of them comes with their own strengths and weaknesses. Based on the review of the latest work, this paper presents a new technique in mitigating node cloning in wireless sensor network, called the Chain Identity Attestation (CIA) method.

IV. METHODOLOGY

We have begun our research by conducting literature review. We have derived our hypothesis from the previous work done on node cloning issues in wireless sensor network and the method developed to prevent node cloning. From the previous studies, issues arise from node cloning are investigated and the flaws of the previous methodologies used are identified. Node cloning is the most common problem in WSN due to security leak in the communication. The adversary can capture packet or data when a sensor node transmitting or receiving the packet. After that the adversary will act as a real node to join as legitimate sensor node in the WSN. Thorough review demonstrated that the leak of the security protocol is the main problem. The attacker can interrupt the protocol during communication, which warrants the enhancement and reinforcement of the security protocol. CIA is one of the methods to prevent node cloning. During the formulation of CIA, the trusted base station is required to store all of the information. In CIA, the identity on the protocol will always change in every session. It is important to change the data to keep the information secured from any attacker. Since the data is always changing, the unique identity is restored inside the node to make it different from others. Moreover, all the changes are independent of each other. After CIA formulation, adversary model is used to verify the CIA. It is to prove that the CIA is valid on preventing node cloning in wireless sensor.

V. CHAIN IDENTITY ATTESTATION METHOD (CIA)

This section will explain on the Chain Identity Attestation Method and how the CIA protects the system from the attackers. figure 1 shows the first stage of CIA method. First stage is done during offline mode and Unique Identity is embedded inside each sensor node. The root of the identity is assumed to be trusted and it is suggested to be kept in a secure encryption memory location.

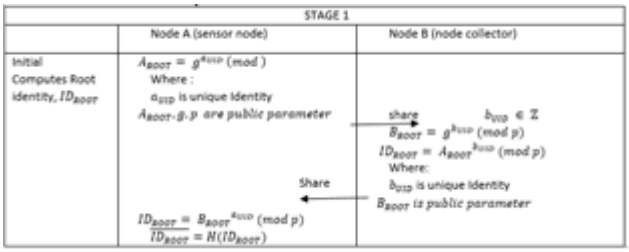

Figure 1: Generation of Root Identity

The second stage is the communication stage. In this stage, all nodes will start to communicate with each other. Both nodes will communicate and exchange their identities. Figure 2 shows the equation involves during node communication. In each session, the identity will be changed in order to avoid node impersonation attack. In CIA, the session identity is computed from its own previous identity, thus been regarded as Chain Identity Attestation (CIA). To keep this Identity from being exposed to any adversary, every session identity is required to be hashed.

In CIA, the identity for both parties will be changed in each session but will depend on the previous data. The session identity is independent and cannot be exposed to others. It is important to keep the session identity private from the environment. Since the session identity depends on the session private identity for each session, the session private identity and unique identity cannot be measured. It is because of the session identity has been hashed. By hashing the session identity, we can protect the unique identity from the attacker even though they are aware of the previous information.

Next stage is the verification part. In this stage, both nodes are required to be verified by a common protocol in order to communicate with the trusted node. Figure 3 shows the method of CIA doing their verification for clone node or

trusted node. If the verification process is successful, it will pass to the next session but if the verification does not match, the node will reject to communicate with the other node. This verification process will repeat for each session of the communication.

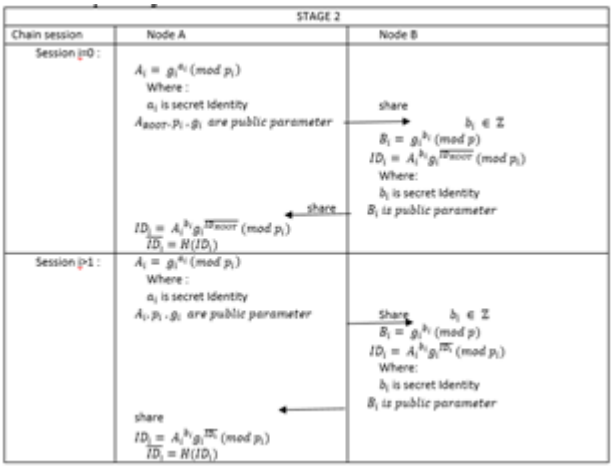

Figure 2: CIA computes during session communicate

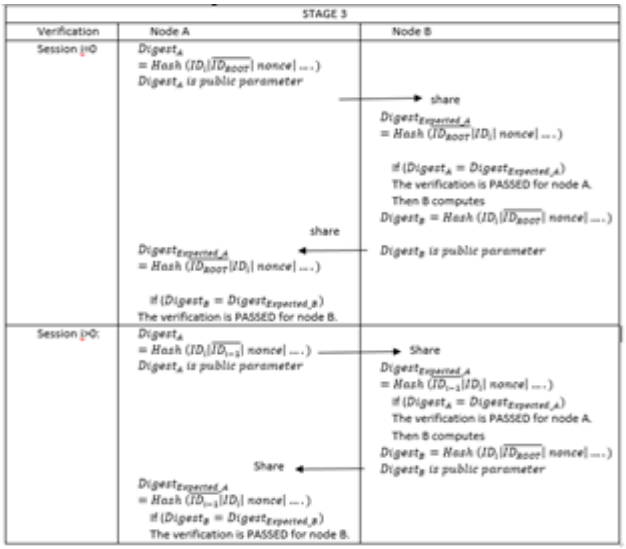

Figure 3: CIA verification session during communicate

VI. Security Analysis

The proposed CIA method is verified using perfect forward attack model, a mathematically-proven method. Perfect forward secrecy attack model consists of four sections which are:

A. Session State Reveal Attack

An adversary (e.g. cannot compute session because the root identity is not accessible to the adversary. The adversary manages to know and but it cannot compute because is unknown. A formalism of the adversary model are:

Adversary model: Session state revel attack
Public knowledge: P_i, g_i, A_i, B_i.
Leaked secret knowledge: $\boldsymbol{a_i, b_i}$
Adversary limitation: The adversary cannot access secret parameters a_{UID}, b_{UID}, ID_{ROOT} because they were embedded in the sensor nodes during installation.
We assume that the adversary cannot access or tamper physical sensor nodes.
Adversary goal: To find $ID_{i=1}$ or ID_{i+1}
Adversary computation:
To find $ID_{i=1}$, Let i=1:
$P_i, g_i, A_i, B_i, ID_i, a_i, b_i \in \mathbb{Z}^*_{n=2048\ bits}$
$\overline{ID_{ROOT}} \in \mathbb{Z}_{n=SHA3\_256\ bits}$
Either:
$ID_i = A_i^{\boldsymbol{b_i}}\ g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$ or
$ID_i = B_i^{\boldsymbol{a_i}}\ g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$
Computes:
$ID_i' = \left[A_i^{b_i}\right] g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$ [1]
When $\overline{ID_{ROOT}}$ is unknown, a probability to find the correct $\overline{ID_{ROOT}}$ using brute force is $\frac{1}{2^{256}}$ such that $ID_i = ID_i'$.
To find $ID_{i=i+1}$, Let:
$P_{i+1}, g_{i+1}, A_{i+1}, B_{i+1}, ID_{i+1}, a_{i+1}, b_{i+1} \in \mathbb{Z}^*_{n=2048\ bits}$
$\overline{ID_i} \in \mathbb{Z}_{n=SHA3\_256\ bits}$
Either:
$ID_{i+1} = A_{i+1}{}^{\boldsymbol{b_{i+1}}}\ g_{i+1}{}^{\overline{\mathrm{ID}_i}} (mod\ P_{i+1})$ or
$ID_{i+1} = B_{i+1}{}^{\boldsymbol{a_{i+1}}}\ g_{i+1}{}^{\overline{\mathrm{ID}_i}} (mod\ P_{i+1})$
Computes:
$$ID_{i+1}{}' = \left[A_{i+1}{}^{b_{i+1}}\right] g_{i+1}{}^{\overline{\mathrm{ID}_i}} (mod\ P_{i+1})$$
When $\overline{ID_i}$ is unknown, a probability to find the correct $\overline{ID_i}$ using brute force is $\frac{1}{2^{256}}$ such that
$ID_{i+1} = ID_{i+1}{}'$.
Security assumption: 1) Computational Diffie-Hellman (CDH) problem is hard in a cyclic group G and 2) hash function is a universal one-way hash function with strong collision-resistant (Mohd Anuar Mat Isa et al., 2015).
Security argument: The session ID_i is secure against the session state revel attack if and only if the adversary A is not able to find $ID_{i+1}\ such\ that\ ID_{i+1} = ID_{i+1}{}'$ with negligible advantage.

[1] The symbol [ ] shows that a given algebra is computable by an adversary.

B. Forward Secrecy

If the adversary manages to know the previous session secrets identity, they still cannot compute the current session key. When adversary manages to know the identity parameter session previously in and but cannot compute because of the current session on are unknown, the formulated of adversary model as below:

Adversary model: Forward secrecy
Public knowledge: $P_{i-1}, g_{i-1}, P_i, g_i, A_i, B_i$.
Leaked secret knowledge: $\boldsymbol{a_{i-1}, b_{i-1}, ID_{i-1}}$
Adversary limitation: Adversary cannot access the secret identity a_i, b_i because the Protocol data is protected using hashing measurements.
Adversary goal: To find current session ID_i
Adversary computation:
To find $ID_{i=2}$, Let i=2:
$P_{i-1}, g_{i-1}, A_{i-1}, B_{i-1}, ID_{i-1}, a_{i-1}, b_{i-1} \in \mathbb{Z}^*_{n=2048\ bits}$
$\overline{ID_{ROOT}} \in \mathbb{Z}_{n=SHA3\_256\ bits}$
Either:
$ID_i = A_i^{\boldsymbol{b_i}}\ g_i^{\overline{\mathrm{ID}_{i-1}}} (mod\ P_i)$ or
$ID_i = B_i^{\boldsymbol{a_i}}\ g_i^{\overline{\mathrm{ID}_{i-1}}} (mod\ P_i)$
Computes:
$[ID_{i-1}] = A_{i-1}{}^{b_{i-1}} g_{i-1}{}^{\overline{ID_{i-2}}} (mod\ p_{i-1})$
$[\overline{ID_{i-1}}] = H(ID_i)$
$ID_i' = A_i^{\boldsymbol{b_i}}\ g_i^{\overline{[ID_{i-1}]}} (mod\ P_i)$
When b_i is unknown, a probability to find the correct ID_i using brute force is $\frac{1}{2^{2048}}$ such that $ID_i = ID_i'$.
Security assumption: 1) Computational Diffie-Hellman (CDH) problem is hard in a cyclic group G and 2) hash function is a universal one-way hash function with strong collision-resistant (Mohd Anuar Mat Isa et al., 2015).
Security argument: The session ID_i is secure against the forward secrecy attack if and only if the adversary $A\ and\ B$ is not able to find $ID_i\ such\ that\ ID_i = ID_i'$ with negligible advantage

C. Key Independence

Based on the forward secrecy model, the session identity is protected even though the adversary manages to discover the previous session parameters. This is because the session

identity is computed independently from all of the previous session information. Even when the adversary manages to attack one session identity using the previous information, it still cannot be used because the previous session identity cannot be reused. Formulations of the adversary model are as described below:

Adversary model: Key independence (or session independence)
Adversary knowledge: $P_{i-1}, g_{i-1}, P_i, g_i, A_i, B_i$.
Leaked secret knowledge: $\boldsymbol{a_{i-1}, b_{i-1}, ID_{i-1}}$,
Adversary limitation: Adversary cannot access the identity parameter a_i, b_i because the Protocol data is protected using hashing measurements.
Adversary goal: To find ID_i from ID_{i-1}
Adversary computation:
To find $ID_{i=1}$, Let i=1:
$P_i, g_i, A_i, B_i, ID_i, a_i, b_i \in \mathbb{Z}^*_{n=2048\ bits}$
$\overline{ID_{ROOT}} \in \mathbb{Z}_{n=SHA3\_256\ bits}$
Either:
$ID_i = A_i^{\boldsymbol{b_i}}\, g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$ or
$ID_i = B_i^{\boldsymbol{a_i}}\, g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$
Computes:
$[ID_i{}'] = \left[A_i^{b_i}\right] g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$
When $\overline{ID_{ROOT}}$ is unknown, a probability to find the correct $\overline{ID_{ROOT}}$ using brute force is $\frac{1}{2^{2048}}$ such that $ID_i = ID_i{}'$.
To find $ID_{i=2}$, Let i=2:
$P_{i-1}, g_{i-1}, A_{i-1}, B_{i-1}, ID_{i-1}, a_{i-1}, b_{i-1} \in \mathbb{Z}^*_{n=2048\ bits}$
$\overline{ID_{ROOT}} \in \mathbb{Z}_{n=SHA3\_256\ bits}$
Either:
$ID_i = A_i^{\boldsymbol{b_i}}\, g_i^{\overline{\mathrm{ID}_{i-1}}} (mod\ P_i)$ or
$ID_i = B_i^{\boldsymbol{a_i}}\, g_i^{\overline{\mathrm{ID}_{i-1}}} (mod\ P_i)$
Computes:
$[ID_{i-1}] = A_{i-1}{}^{b_{i-1}} g_{i-1}{}^{\overline{ID_{i-2}}}\ (mod\ p_{i-1})$
$[\overline{ID_{i-1}}] = H(ID_{i-1})$
$ID_i{}' = A_i^{\boldsymbol{b_i}}\, g_i^{\overline{[ID_{i-1}]}} (mod\ P_i)$
When b_i is unknown, a probability to find the correct ID_i using brute force is $\frac{1}{2^{2048}}$ such that $ID_i = ID_i{}'$.
When probability to find $ID_i = ID_i{}'$ is negligible, then it will reflex a negligible correlation between ID_i and ID_{i-1}.
Therefore, ID_i *and* ID_{i-1} are independent and not related to each other.
Security assumption: 1) Computational Diffie-Hellman (CDH) problem is hard in a cyclic group G and 2) hash function is a universal one-way hash function with strong collision-resistant (Mohd Anuar Mat Isa et al., 2015).
Security argument: The session ID_i is secure against the key independence if and only if the adversary A *and* B is not able to find ID_i *such that* $ID_i = ID_i{}'$ with negligible advantage.

D. Key Derivation Function Attack

To prevent key derivation function attack, the session identity is hashed during message transfer and there is no relation between session identity and future session identity. When the public parameters were known by an adversary, it cannot compute or . The adversary cannot break the identity because algebraic relations between session identity and future session identity are eliminated. Therefore, no correlation between session identity and future session identity. Formulation of adversary model:

Adversary model: Key derivation function attack
Adversary knowledge: P_i, g_i, A_i, B_i
Leaked secret knowledge: $\boldsymbol{a_i, b_i, ID_{i-1}}$,
Adversary limitation: The adversary cannot access secret parameters ID_i because it convert to $\overline{ID_i}$.
Adversary goal: To find $g^{\overline{ID_{ROOT}}}$ and $g^{\overline{ID_{i-1}}}$
Adversary computation:
To find $ID_{i=1}$, Let i=1:
$P_i, g_i, A_i, B_i, ID_i, a_i, b_i \in \mathbb{Z}^*_{n=2048\ bits}$
$\overline{ID_{ROOT}} \in \mathbb{Z}_{n=SHA3\_256\ bits}$
Either:
$ID_i = A_i^{\boldsymbol{b_i}}\, g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$ or
$ID_i = B_i^{\boldsymbol{a_i}}\, g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$
Computes:
$[ID_i{}'] = \left[A_i^{b_i}\right] g_i^{\overline{\mathrm{ID}_{ROOT}}} (mod\ P_i)$
When $\overline{ID_{ROOT}}$ is unknown, a probability to find the correct $\overline{ID_{ROOT}}$ using brute force is $\frac{1}{2^{2048}}$ such that $ID_i = ID_i{}'$.
To find $ID_{i=2}$, Let i=2:
$P_{i-1}, g_{i-1}, A_{i-1}, B_{i-1}, ID_{i-1}, a_{i-1}, b_{i-1} \in \mathbb{Z}^*_{n=2048\ bits}$
$\overline{ID_{ROOT}} \in \mathbb{Z}_{n=SHA3\_256\ bits}$
Either:
$ID_i = A_i^{\boldsymbol{b_i}}\, g_i^{\overline{\mathrm{ID}_{i-1}}} (mod\ P_i)$ or
$ID_i = B_i^{\boldsymbol{a_i}}\, g_i^{g^{\overline{\mathrm{ID}_{i-1}}}} (mod\ P_i)$
Computes:
$[ID_i] = \left[A_i^{b_i}\right] g_i^{\overline{ID_{i-1}}}\ (mod\ p_i)$
$\overline{ID_i} = H(ID_i)$
$ID_i{}' = A_i^{\boldsymbol{b_i}}\, g_i^{\overline{ID_{i-1}}} (mod\ P_i)$
When $\overline{ID_{i-1}}$ is unknown, a probability to find the correct ID_i using brute force is $\frac{1}{2^{2048}}$ such that $ID_i = ID_i{}'$.
Security assumption: 1) Computational Diffie-Hellman (CDH) problem is hard in a cyclic group G and 2) hash function is a universal one-way hash function with strong collision-resistant (Mohd Anuar Mat Isa et al., 2015).
Security argument: The session ID_i is secure against the session state revel attack if and only if the adversary A is not able to find ID_{i+1} *such that* $ID_{i+1} = ID_{i+1}{}'$ with negligible advantage
The Adversary advantages to mount the session state reveal attack, forward secrecy, key independence and key derivation function attack as below:
Probabilistic polynomial-time (PPT)[2] to determine value 0 or 1 for solving CDH hard problem in a random oracle model.

$$Adv_A^{CDH} = \Pr[A(g, g^a, g^b, g^{\overline{ID}}, g^{ab\overline{ID}}) = 1 : (a, b \in \mathbb{Z}^*_{n=2048}, \overline{ID} \in \mathbb{Z}_{n=SHA3_{256bits}})]$$

Adv_A^{CDH} **is** negligible based on the above security assumption.

[1] "polynomial-time" is a term used for measuring an algorithm's running time as a function, wherein it is measured by length of its input into the function (Mohd Anuar Mat Isa et al., 2015). E.g. function $f(x)$ take $x = 2048$ as input string during execution, then the running time is x.

VII. CONCLUSION

We present our chain identity method in preventing node cloning attack in wireless sensor network and we have succeeded to fulfill the objective and demonstrated cryptographic computation capability. We are assertive with the perfect forward secrecy attack model used to proof our new CIA attestation method. Future paper will present the analysis on the energy utilization and communication overhead.

ACKNOWLEDGMENT

The authors would like to acknowledge the Ministry of Education (MOE) Malaysia for providing the grant 600-127/RMI/FRGS 5/3 (108/2014) and Universiti Teknologi MARA (UiTM) for supporting this research work.

REFERENCES

[1] Mohd Anuar Mat Isa, Habibah Hashim, Jamalul-lail Ab Manan, Syed Farid Syed Adnan, Ramlan Mahmod, "Cryptographic Adversary Model: Timing and Power Attacks", *Trans. Eng. Technol. Springer*, 2015.
[2] Kalita, H. K. and Kar, A., W s n s a., 1(1), 2009, pp.1–10.
[3] Sharma, R., Chaba, Y. & Singh, Y., "Analysis of Security Protocols in Wireless Sensor Network", *International Journal of Advanced*, vol.713, 2010, pp. 707–713.
[4] Mohammadi, S. and Jadidoleslamy, H., "A comparison of physical attacks on wireless sensor networks", *International Journal of Peer to Peer Networks*, vol.2, no.2, 2011, pp.24–42.
[5] Udgata, S.K., Mubeen, a & Sabat, S.L., "Wireless Sensor Network Security Model Using Zero Knowledge Protocol", *Communications (ICC), 2011 IEEE International Conference*, 2011, pp.1–5.

[6] Capkun, S. and Hubaux. J. -P., "Secure positioning of wireless devices with application to sensor networks", *Infocom*, vol.313, no.3, 2005, pp. 1917–1928.

[7] Ding, M. et al., 2005. Localized fault-tolerant event boundary detection in sensor networks. Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. 2.

[8] Kyasanur, P. and Vaidya, N. H., 2003. Detection and Handling of MAC Layer Misbehavior in Wireless Networks. Proceedings of the International Conference on Dependable Systems and Networks.173–182.

[9] Xing, K. X. K. et al., "Real-Time Detection of Clone Attacks in Wireless Sensor Networks", *2008 The 28th International Conference on Distributed Computing Systems*, 2008, pp.3–10.

[10] Boneh, D. and Franklin, M., Zhu, W.T., "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme", *2011 International Conference on Network Computing and Information Security*, vol. 2, 2003, pp.156–160.

[11] "Identity-Based Encryption from the Weil Pairing", *SIAM Journal on Computing*, 32, pp.586–615.

[12] Lyubashevsky, V., "Lattice-Based Identification Schemes Secure", 2008, pp.162–179.

[13] Mandal, S. and Mohanty, S., "Multi-party Key-Exchange with Perfect Forward Secrecy", *2014 International Conference on Information Technology*, 2014, pp.362–367.

[14] Leu, J.-S. and Hsieh, W.-B., "Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards", *IET Information Security*, 2014, pp.104–113.

[15] Li, Z. and Gong, G., "On the Node Clone Detection in Wireless Sensor Networks", vol.21, no.6, 2013, pp.1799–1811.

[16] Lee, C.C., Lai, Y.M. & Li, C.T., "An improved secure dynamic ID based remote user authentication scheme for multi-server environment", *International Journal of Security and its Applications*, vol.6, no.1, 2012, pp.203.