Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

TWO PHASES AUTHENTICATION LEVEL (TPAL) PROTOCOL FOR NODES AUTHENTICATION IN INTERNET OF THINGS

M. F. Razali*, M. E. Rusli, N. Jamil, S. Yussof

College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia

Published online: 01 February 2018

ABSTRACT

Nodes are required to be authenticated in order for them to join the network nodes especially for Low power and Lossy Network (LLN). The purpose of authentication is to verify the claimant is really what it claims to be. Since LLN made up from many nodes, some of the node may contain sensitive informations such as military data and monitoring data. Therefore, any packets forwarded by a node may need authentication at the source and destination nodes. LLN is a kind of Internet of Things (IoT) network with limited power source due to the fact they running on battery, low processing capability, have high data loss and low data rate. Current authentication Internet protocols cannot be adopted directly into LLN due to its characteristics. For now, LLN rely on the authentication provided by Routing Protocol for LLN (RPL) which is based on symmetric cryptography. However, RPL specification stated thatany node that wants to act properly as a router by using the authenticated mode in RPL should not be based on symmetric cryptography. A two phase authentication level (TPAL) is proposed in this paper to improve the authentication mode used in RPL. The proposed protocol contains two parts mainly for system initialization and node authentication phase with the help from a trusted party. The authentication takes place during node discovery which is guided by the routing protocol thus only those nodes in the data path will be authenticated.

Keywords: LLN, RPL, verification, ECC, lightweight, scheme

Author Correspondence, e-mail: techfree91@gmail.com

doi: http://dx.doi.org/10.4314/jfas.v10i2s.16

1. INTRODUCTION

In the Internet of Things (IoT), any physical objects or nodes that encompass us in day to day life will be associated with a network. With the rapid development of these associated intelligent nodes, they impose a great challenge especially in the routing and authentication protocol due to the fact that typically, nodes running in IoT are battery powered. Therefore, any routing or authentication protocol to be established needs to address this issue. In the meantime, the Routing Over Low-power and Lossy Networks (ROLL), a group from Internet Engineering Task Force (IETF) has been established to work on this area. Basically, according to ROLL group, Low-power and Lossy Networks (LLNs) consists of resource constrained routers and interconnect nodes [1]. In addition, its network behavior and traffic patterns are not just simply point to point but also include point to multipoint or multipoint to point.

In general, LLNs comprise of many embedded nodes with constrained power, memory and processing assets. These networks are interconnected by an assortment of connections, for example, IEEE 802.15.4, Bluetooth, Low Power WiFi, wired or other low power (i.e. Powerline Communication) links [2]. These interconnections are often portrayed as having high data loss, low data rate, and usually unstable delivery rate. The attributes of LLNs determine the network security dangers, the security framework and security algorithms that are not the same as those in standard conventional networks [3]. Consequently,the conventional network security frameworks and security algorithms cannot be adopted directly.

Symmetric encryptions are a common choice to be utilized in LLN due to the energy and processing power limitations of nodes[4]. Nodes may share the same key among them which simplifies the key management but this will cause vulnerability to the whole network if any node happened to be compromised. On the other hand, each pair of nodes may share a distinct key. If others have a knowledge about that particular key, only those pair will be compromised. For a big network, we need to store a very large amount of keys and thus will make the key management become complicated. In this way, utilizing this authentication technique in the large size of LLN will cause poor system expandability.

Public Key Cryptography (PKC) has the feasibility to be adapted into Wireless Sensor Network (WSN) as proved by numerous researchers that include node authentication protocol [5] that incorporated the Elliptic Curve Cryptography (ECC) and XKAS Key Agreement Scheme to enhance the scheme proposed by X. Huaping [6]. Their studies showed that PKC has a remarkable authentication reliability, which can avert security threat such as the Man-In-The-Middle attack.

Table 1. The key length ratio between ECC, RSA and DSA [5]

Key Length of RSA/DSA	Key Length of ECC	Key Length Ratio of RSA/ECC
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

Nowadays, ECC has become a popular choice to be adopted since the key length is quite short compared to other public encryption while providing the same security protection. ECC also provides more advantages such as lower bits length for key size, higher intensity, and fewer parameters. Thus, ECC is more compatible to be used for constrained nodes as compared to RSA. Table 1 shows the key lengths of three cryptographic methods under the same security and the ratio of RSA to ECCkey length [5]. For example, the 512 key lengths of RSA compared with 106 key lengths of ECC are equivalent to 5:1, which means that 106 ECC provided the same security level with 512 RSA.

Since nodes in LLN are resources constraint, authentication becomes more challenging. Besides, RFC6550 for Routing Protocol for LLN (RPL) also highlights that the authentication mode must not be based on symmetric cryptography and still in reserve for future work [1]. As such, there is a need for a convenient and lightweight authentication protocol [7]. In this paper, a two phases authentication level (TPAL) protocol which is based on ECC using a trusted party which is applicable to LLN is proposed as shown in Figure 2 and 3. We also suggest that key disclosure and key graph constructionbe guided by the routing protocol which in this case is RPL. Therefore, nodes will attempt to find the rightful owner of the public keys while finding routing path. This can be accomplished by coordinating the key discovery phase and as the result, the construction of the key graph in the routing algorithm.

Hence, we propose a lightweight authentication protocol that empowers node to find the proprietor of the public keys broadcast by the trusted party while authenticating them to each other. Besides, we also compared the efficiency of the TPAL in terms of message complexity. Later, we will simulate the protocol using an automated security protocol analysis tool known as SPAN-AVISPA, which is a powerful tool that finds attacks for defined protocol properties as we discussed in Section 4.

The rest of the paper is organized as follows. The following section which is Section 2 presents the related work. Meanwhile in Section 3, we explain our proposed authentication

protocol followed by the discussion on our protocol assessment and efficiency analysis in Section 4. Lastly, this paper is concluded in Section 5.

2. RELATED WORK

Usually, LLNs are comprised of multiple nodes with constrained resources distributed and located around the places that could be at urban area or industrial area. These nodes are always left attended and running on battery powered. Most Internet security protocols are computationally expensive and cannot be adopted directly to the resource limited LLNs[3]. Past researchers have proposed several authentication protocols [3-7,9-16] that provide security in a LLNs environment. However, for LLNs, symmetric cryptography acts as a norm due to its limitations on node resources [4]. Essentially, it is crucial to design an efficient, secured and lightweight authentication mechanism due to the facts that nodes have low computational time, storage, and communication capabilities.

The LLN's network with RPL in this article is shown in Figure 1. RPL is designed to provides solution for nodes with resources constrained in LLN's by reducing the control traffic thus minimizing the overall power consumption. But, RPL lacks of security mechanism in Authenticated Mode in order to provide security support for node that intents to be a router. RPL standard clearly stated that this operation should not be supported by symmetric cryptography but at the same time does not mention on how it can be adopted.

In 2015, Santoso presented an approach to incorporate ECC to perform authentication for smart home system [7]. This approach is based on protocol proposed by Martin [8] without the need of a trusted party in order to reduce the power and energy consumption. Later, the mobile device can be used to further make the authentication process much easier for devices with restricted user interface. Our protocol, TPAL is an enhance version from Martin protocol with a trusted party to help facilitate the authentication between nodes. TPAL uses ECC due to the fact that it can provides the same security level of RSA while having a lower key size. Furthermore, the pre-shared secret keys (K) install in the program prior to the distribution of nodes may remove the need to have another security layer for the protocol.

Our protocol, TPAL allows the nodes and the trusted party to establish authentication connections with different nodes that belong to the group. Furthermore, the authentication is also guided by the RPL in terms of nodes discovery thus can reduce energy consumption. TPAL will also enhance the security mode option provided in RPL [1] which makes our protocol suitable to be deployed in the future in order to support the emerging technologies of IoT. The TPAL protocol comprises of two phases. The first is for the distribution of the public keys

among the nodes and the trusted party. This eliminates any malicious nodes that try to insert itself into the network even though their keys do not belong in this setup. The second part is for the nodes to authenticate themselves.

3. PROPOSED PROTOCOL

There are certain criteria that we follow when we design the protocol:

- The network is made up of a large number of battery powered nodes.
- No nodes assume special role except for the routing node.
- We assume the communication between Trusted Party (TP) and nodes are secured.
- Nodes are required to hash their unique identity to reduce storage overhead.

Our protocol is meant to enable a TP to distribute the keys via asecure channel to the neighbor nodes and therefore, each node will authenticate each other. The proposed authentication protocol for LLN applications encompasses of two phases where theinitial stage is to acquire security accreditations from TP.

Meanwhile, the second stage is where it beginsto authenticate between nodes, utilizing the security accreditations. Figure 2 shown the abstract view of our proposed protocol. The protocol architecture identifies security services needed to meet the secure protocol requirement such as confidentiality, integrity, and non-repudiation.

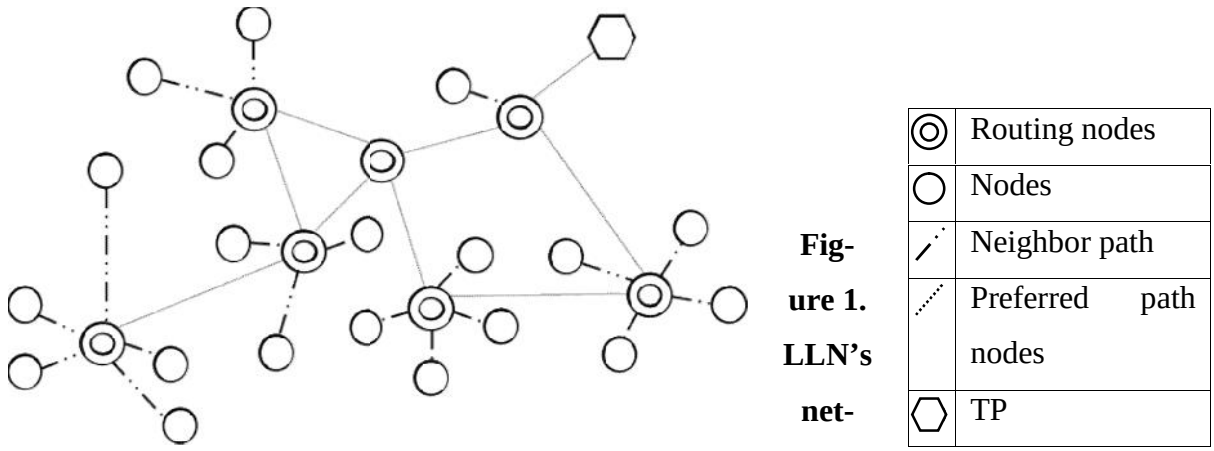

Figure 1. LLN's network.

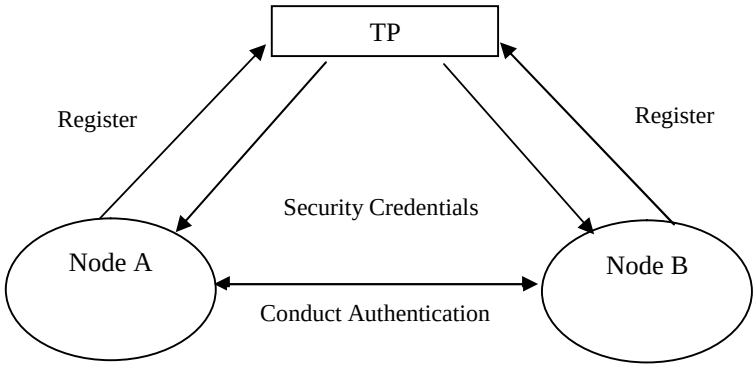

Fig.2. Abstract view of proposed protocol architecture

Table 2. The Notation Used Throughout the Paper

Message	Meaning
A, B…	Node names
TP	Trusted party
E[m]	Encrypt message m
X_{k1}, X_{kn}	Public key stored in node
H(A)	Node A hashed value
Sig_A, Sig_B	Signature of node A, node B
A → B : m	A sends to B message m

Table 2 highlights the notation that we use in protocol descriptions. Node A stores *n* keys received from TP and will run a mutual authentication with node B.

.

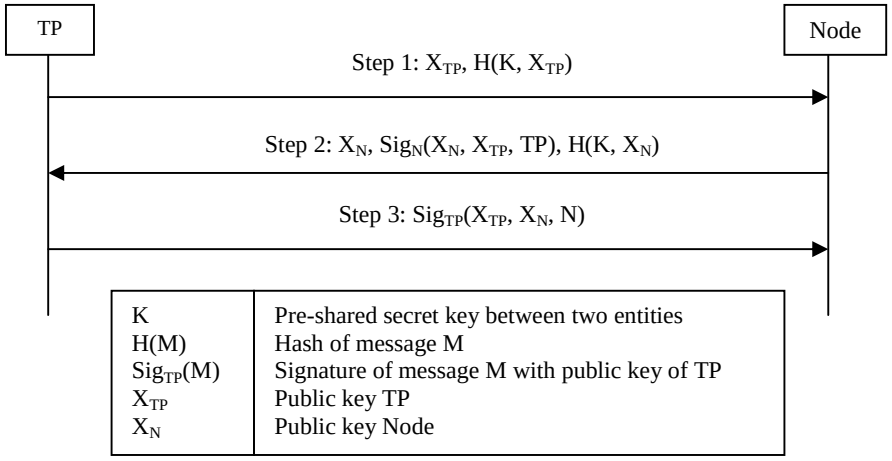

Fig.3. Authentication use between TP and nodes [8]

In the first part of this protocol, it only involves the nodes and TP. Each node is required to register them at TP. Any nodes whose hashed ID is not in the pre-stored ID table will be considered as an illegal node. ECC will be adopted to maintain lightweight properties and TP generates keys for each node.

After system initialization, TP distributes the private keys for each node and all known hashed IDs using the approach as shown in Figure 3[8] while broadcasting the public keys to all nodes. Nodes capture these public keys in order for them to mutually authenticate with other nodes. The information regarding the hashed ID will be used to verify the authentication.

In the second part, TP will act as a verifier of node authentications. Node A sends A1 which contains information of its hash value of its ID and public key with its public key to node B. B will store the information and send back the message from A to TP including B's information too. TP will verify that information from A and B is indeed from them. If TP acknowledges both of them really belong to TP's group, it will send the signed message which contains both nodes public keys and its public key to node B. This is to inform node B that node A is really, what it claims to be and also the one to attempt the authentication. If not, TP will disregard the message.

If the claim is successful, B will then send the message to node A which contains its signed hash ID and public key with node A's public key. Node B too will send a sign message to TP which contains both public keys and hash value of its ID and node A's ID. If node A replies with signed message containing the same message of what node B send to TP, then authentication can be considered successful. Now, presently both A and B are authenticated to each other. Figure 4 shows the protocol steps.

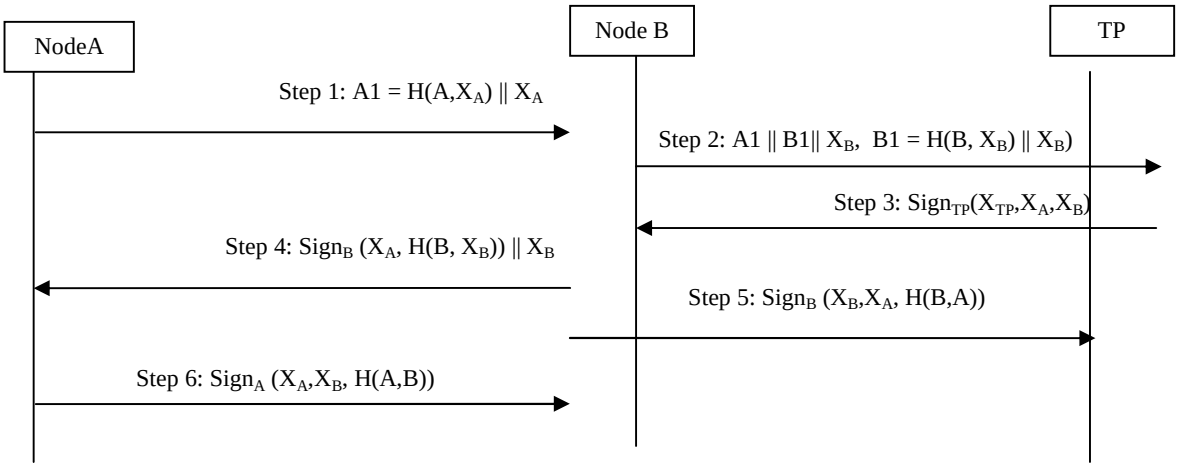

Fig.4. Authentication between nodes

4. ANALYSIS

We provide an informal analysis of the proposed protocol. The proposed protocol is claimed to achieve security properties which are confidentiality, secrecy and integrity. Moreover, level of security and efficiency are two metrics that contradict with each other with regards to lightweight authentication protocol. In general, the higher the level of security, the more likely that the program to have a lower efficiency in terms of program execution such as simplicity, message complexity and time synchronization. As for this paper, it is important to have an

adequate security and efficiency, especially for resource constrained nodes. By efficiency, we define it as message complexity.

1. Every node stores its own private key and this will not be revealed even when the TP is under attack. Once TP successfully broadcast the public keys, it will refresh the table and thus contains only the hashed value of legal nodes. If the private key is untrusted, TP may restart the process by reselecting the new private key. In order for amalicious node to join the network, it is required for the node to insert its ID into the TP table. Thus, this protocol achieves confidentiality.

2. An attackermayintercept the public keys but without knowing the specific owner of the keys will only make the keys harder to crack. Since ECC is used here, it is probably hard for the attacker to get the private keys. Thus the attacker cannot disguise himself as one of the legal nodes to accomplish authentication with another node. He may use its own public key in order to gain access to the network. Since this protocol requires to check the ID to be compared between the node, the authentication process will stop if it acknowledges that ID does not belong to the network. Therefore, this protocol can resist active attack and eliminate the change of identity.

3. Even when the attacker falsified the *A1 or B1* information, the message will become useless since it will be verified by TP. Thus, the authentication process will be dropped immediately. This method also achievesnon-repudiation as signature is used throughout here in this scheme.

4. If the decryption is successful, the node needs to check the other's ID hashed value before it can proceed to the next step. Due to the fact that the node's ID is a unique one which cannot be duplicated, this protocol can oppose the man in the middle attack.

5. Any attacker cannot unscramble the hashed value since hash function is sort of a one-way irreversible function. Therefore, any node that stores the ID hash value can disguise the node's genuine identity. This achieves integrity.

In our proposed protocol, we assume that cryptographic hash (H) and asymmetric encryption or decryption processes have similar message complexity to $E[m]$ where m is the size of the message while X is for XOR operation. Thus the efficiency will determine the TPAL's performance. The unicast message (UC) requires $2E$ operations for both encrypt and decrypt while broadcast message (BC) requires $(N+1)E$. From the whole execution of the protocol, the message complexity is determined by each process equal to 1 as shown in Table 3.

Table 3. Node Processes Involving Message Operation Protocol

Protocol	Phase	Message Complexity	Communication Complexity	Time Synch
TPAL	Registration	4*E*, 2*H*	3*UC*	-
	Authentication	8*E*, 4*H*	6*UC*	-
AKMS [9]	Registration	(2+*N*)*E*, 1*H*	1*BC*	-
	Authentication	4*E*, 3*H*	3*UC*	-
Y. Lu et al. [10]	Registration	4*E*, 10*H*, 2*X*	2*UC*	-
	Authentication	8*E*, 17*H*, 15*X*	4*UC*	3*T*
Farash et al. [11]	Registration	4*E*, 6*H*, 2*X*	2*UC*	2*T*
	Authentication	30*H*, 16*X*	4*UC*	4*T*

From Table 3, the message complexity of TPAL in both registration and authentication is slightly expensive compare to AKMS[9]. But TPAL outperforms both Y Lu et al. [10]. and Farash et al. [11].AKMS is the most efficient followed by TPAL as AKMS is based on symmetric encryption scheme in [3] with different key scheme while TPAL is asymmetric encryption. The messages involved here are acceptable and TPAL does not require the use of time synchronization between the trusted party and nodes as compare to [12] scheme.

Node stores the others node's ID hash value and thus reduces the need for larger memory allocation. It also stores the available legal nodes' public keys. This protocol is also lightweight as no sorting or reversing technique is used.

The limitation of TPALis mostly dictated by the low resources of nodes in LLN. A subsequent bottleneck of the execution of this protocol is the computation of encrypting each message using available public keys by both nodes happen during the second part of this authentication. The same goes to node B during the step that requires it to encrypt the signed message using all keys known to it.

5. CONCLUSIONS

In this paper, we propose a lightweight authentication protocol, TPAL, using public key encryption and a trusted party. TPAL is designed to be lightweight by making use the combination of hash function and ECC. Furthermore, nodes only need to store others ID's hash value and thus reduce the storage consumption. Besides, the authentication is guided by the routing protocol in terms of node discovery during routing path discovery. Thus, anodethat does not

involve in the process mentioned above may not necessary to authenticate itself with every one of its neighbors and hence can reduce energy consumption. Future research will focus on the simulations using Contiki and the real testbed may be carried out in order to reflect the actual performance of TPAL. This protocol will also be compared against well-known authentication protocols.

6. ACKNOWLEDGMENTS

This work was supported by the Ministry of Higher Education (MOHE) under the Fundamental Research Grant Scheme (FRGS). We would like to express thanks to the fellow researchers of College of Computer Science and Information Technology (CSIT), UNITEN. This paper would not have been possible without their support.

7. REFERENCES

[1] W. T. Ed, T. P. Ed, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *Internet Engineering Task Force (IETF) RFC 6550,* 2012.

[2] I. Robbles, P. Van der Stok, A. Retana, M. Richardson, R. Cragie and Y.-A. Pignolet, "Routing Over Low power and Lossy networks (roll)," 9 June 2017. [Online]. Available: https://datatracker.ietf.org/wg/roll/about/.

[3] O. D. Mohatara, A. F. Sabatera and J. M. Sierra, "A Lightweight Authentication Scheme for Wireless Sensor Networks," *Journal of Ad Hoc Networks,* pp. 727-735, 2011.

[4] B. David and N. Thomas, "Securing Wireless Sensor Network: Ssecurity Architectures," *Journal of Networks,* pp. 65-77, 2008.

[5] Q. Chang, Y.-p. Zhang and L.-l. Qin, "A Node Authentication Protocol based on ECC in WSN," *ICCDA,* pp. 606-609, 2010.

[6] X. Huaping and W. Zhongbao, "Design and implementation of identity authentication system based on ECC," in *Control and Automation*, 2007.

[7] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *IEEE International Symposium on Consumer Electronics (ISCE)*, Madrid, 2015.

[8] M. Noack, "Optimization of Two Way Authentication Protocol in Internet of Things (MasterThesis)," 2014. [Online]. Available:

https://files.ifi.uzh.ch/CSG/staff/schmitt/Extern/Theses/Martin_Noack_MA.pdf.

[9] D. Qin, S. Jia, E. Wang and Q. Ding, "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Network," *Journal of Sensors,* vol. 2016, p. 9 pages, September 2016.

[10] Y. Lu , L. Li , H. Peng and Y. Yang, "An Energy Efficient Mutual Authentication and Key Agreement Scheme Preserving Anonymity for Wireless Sensor Networks," *Sensors,* vol. 16, no. 6, p. 837, June 2016.

[11] M. S. Farash, M. Turkanović, S. Kumari and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks,* vol. 36, pp. 152-176, January 2016.

[12] Z. Quan, T. Chunming, Z. Xianghan and R. Chunming, "A secure user authentication protocol for sensor network in data capturing," *Journal of Cloud Computing,* vol. 4, no. 6, 2015.

[13] M. Saleh and E. Sourour, "Authentication in Flat Wireless Sensor Networks with Mobile Nodes," in *IEEE 12th International Conference on Networking, Sensing and Control*, Taiwan, 2015.

[14] P. Porambage, C. Schmitt , P. Kumar, A. Gurtov and M. Ylianttila, "Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications," *Wireless Communications and Networking Conference,* pp. 2728-2733, 2014.

[15] S. Guicheng and Y. Zhen, "Application of Elliptic Curve Cryptography in Node Authentication of Internet of Things," *Intelligent Information Hiding and Multimedia Signal Processing*, pp. 452-455, 2014.

[16] S. V. L, R. M. A, M. Singh and B. P, "One Time Password Authentication Scheme based on Elliptic Curves for Internet of Things (IoT)," *IEEE National Symposium on Information Technology:Towards Smart World,* 2015.

How to cite this article:
Razali M F, Rusli M E, Jamil N, Yussof S. Two phases authentication level (tpal) protocol for nodes authentication in internet of things. J. Fundam. Appl. Sci., 2018, *10(2S), 190-200.*