Journal of Computer Science

Original Research Paper

TPAL: A Protocol for Node Authentication in IoT

Mohamad Faiz Razali, Mohd Ezanee Rusli, Norziana Jamil and Salman Yussof

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

Article history
Received: 13-03-2018
Revised: 10-07-2018
Accepted: 26-10-2018

Corresponding Author:
Mohamad Faiz Razali
Universiti Tenaga Nasional,
Putrajaya, Malaysia
Email: techfree91@gmail.com

Abstract: Secure communication in Low power and Lossy Network (LLN) requires the authentication of the identities of nodes for that node to join the network. Since LLN may consist of many different nodes, where some nodes may contain sensitive and subtle information such as military data, monitoring data, or health data, that node needs to be authenticated before it can deliver any data packet. Even though LLN uses an Internet connection, current authentication for Internet protocols cannot be adopted directly into LLN due to LLN's limited resources. LLN relies on the authentication provided by Routing Protocol for LLN (RPL), which is based on symmetric cryptography. Nevertheless, RPL reserves a mode for future work in terms of public cryptography. In this study, we propose an authentication protocol for LLN that utilizes Elliptic Curve Cryptography (ECC) called as TPAL.

Keywords: Verification, Lightweight, Scheme, SPAN-AVISPA, Security

Introduction

Nowadays, we live in an environment surrounded by electronic devices. These devices may be owned by us or other people. With the Internet, these devices become more crucial as they can send any information they may have in our life to any party may it be associated with or not (Dhillon and Kalra, 2017). Some unauthorized node may also collect information on us, and we are unaware of this. Thus, security became apparent as it is important to establish authentication on these devices before they can be connected to the network. Any routing protocol to be established needs to address this issue.

LLNs consist of many resource-constrained routers and interconnect nodes in a self-organized manner where there are no central control nodes (Brandt *et al*., 2012). LLN's connections are often portrayed as having high data loss, low data rate, and usually unstable delivery rate. These characteristics of LLNs which quite different than the network that using an unlimited power source, thus making security, much challenging to be managed (Delgado-Mohatar *et al*., 2011). The limited storage space, computational capabilities, and power supply also make the Internet security frameworks cannot be adopted directly into LLN.

Symmetric encryption is a typical decision to be used in LLN because of the energy and processing power restrictions of nodes (Boyle and New, 2008). It is highly possible with symmetric encryption, nodes may have a similar key among them. This disentangles the key management, but it is highly likely that this will cause network vulnerability if any node happened to be compromised. Then again, each pair of nodes may share a distinct key. If others have thought about that specific key, just those pair will be compromised. In the event of a big network, we need to keep a lot of keys which causes the key management to be complicated. Along these lines, using this authentication technique in the substantial size of LLN will cause poor system scalability.

Asymmetric cryptography has the feasibility to be adopted into Wireless Sensor Network (WSN) as proven by numerous researchers (Guicheng and Zhen 2013; Noack, 2014; Santoso and Vun, 2015; Jiang *et al*., 2016; Li *et al*., 2017). Their studies showed that this type of cryptography has a remarkable authentication reliability, which can avert security threat such as the Man-In-The-Middle attack. The most popular trending of asymmetric cryptography is ECC.

ECC key length is quite short compared to other public encryption while providing the same security protection (Chang *et al*., 2010). A 256-bit ECC key can be considered equivalent to a 3072-bit RSA key. IoT applications which uses RSA keys are quite large and difficult to handle. In order to save power, rather than transmit larger data over a radio link which may result in buffer size problems or causing the data to not fit into a single network packet, another solution is by transmitting as few bytes as possible. Thus, ECC is

more compatible to be used for constrained nodes as compared to RSA.

Since nodes in LLN are resource constraint, authentication becomes highly challenging. RFC6550 for Routing Protocol for LLN (RPL) mentions that the authentication mode must not be based on symmetric cryptography but does not state specifically on how asymmetric cryptography can be utilized here (Brandt *et al*., 2012). In that capacity, there is a need for a convenient and lightweight authentication protocol.

In this study, a Two-Phase Authentication Level (TPAL) protocol which is based on ECC using a trusted party is proposed as shown in Fig. 2 and 3. We suggest that the key disclosure and key graph construction be guided by the routing protocol which in this case is RPL. Therefore, the node will attempt to authenticate its neighbors while finding a routing path by coordinating the key discovery phase.

TPAL is simulated 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 more in section 4. Ziauddin and Martin (2013) mentioned that due to the modular approach used in this tool, AVISPA has been considered as robust. The protocol simulated in AVISPA is written using HLPSL language while a CAS+ can be used to ease the HLPSL specifications (Genet, 2015).

The rest of the paper is organized as follows. The following section presents the related work. Next section presents an explanation of our proposed authentication protocol followed by the discussion on our protocol assessment using AVISPA. The last section is our conclusion.

Related Works

LLNs comprises of multiple nodes with constrained resources ordinarily situated around the spots that could be an urban area or industrial area. These nodes are usually battery powered and often left unattended. Internet security protocols are mostly computationally expensive and thus cannot be adopted directly to the resource-limited LLNs. With the development of security technology in LLN, the research on security protocol has been increasing in recent years and several authentication protocols have been proposed. However, for LLNs, symmetric cryptography acts as a norm due to the limits on the node resources. Basically, it is important to design an efficient, secured and lightweight authentication mechanism due to the facts that nodes have low computational time, storage and communication capabilities. The recent authentication protocol is shown in Table 1 from our previous work (Razali *et al*., 2017).

RPL is designed to provide a solution for nodes with resources constrained in LLN's by reducing the control traffic thus minimizing the overall power consumption. However, RPL lacks security mechanism in its Authenticated Mode to provide security support for a node that intends 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 how it can be adopted.

Table 1: Authentication protocol proposed for IoT

Researchers	Encryption type	Technique
Chang *et al*. (2010)	Asymmetric ECC	XKAS-based Key Agreement Scheme
Liu and Yan (2012)	Symmetric	Exclusion Basis System and keyed-hash functions (HMAC).
Guicheng and Zhen (2013)	Asymmetric ECC	Implementation of ECC into RFID tags and backend system.
Porambage *et al*. (2014)	Asymmetric ECC	Elliptic Curve Qu Vanstone (ECQV) implicit certificate scheme and Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol
Shivraj *et al*. (2015)	Asymmetric ECC	Lightweight identity-based scheme with Lamport's OTP algorithm.
Santoso and Vun (2015)	Symmetric and asymmetric ECC	The user needs to load the IoT's device credential into the mobile device.
Rghioui *et al*. (2015)	Symmetric	Remote server-based authentication and hybrid security keys management.
Banerjee *et al*. (2015)	Symmetric	Lightly computation operation such as Ex-OR, extraction, bitwise shuffle etc. in every part of implementing the algorithm.
Saleh *et al*. (2015)	Symmetric	Authentication is guided by a routing protocol such as SPIN.
Jiang *et al*. (2016)	Asymmetric	An improved version from previous work as a case study for deliver untraceable two-factor authentication protocol.
Bala *et al*. (2017)	Asymmetric	Nodes are not required to execute a public cryptography as this protocol relies on the use of certificate-less public key cryptography.
Hammi *et al*. (2017)	Symmetric	Provide mutual authentication at MAC sub-layer.
Li *et al*. (2017a)	Asymmetric	A lightweight encryption scheme for smart city application
Shen *et al*. (2018)	Asymmetric	A lightweight one to many and Sun protocol based on ECC between PDA and sensor nodes.

Santoso and Vun (2015) presented an approach to use a protocol proposed by Noack (2014) in order to perform the authentication for the smart home system. While each of the IoT devices in the house can only communicate with the home gateway itself, any interaction from one device may trigger the gateway to communicate with another device for the corresponding action. Later, a mobile device can be used to further ease the authentication process for devices with the restricted user interface.

Two-Phase Authentication Level (TPAL) Protocol

In this section, we present an approach for node authentication protocol in LLN. We also discuss certain characteristics that we considered during the protocol development such as:

- The network is comprised of countless battery-powered nodes
- No node accepts special role aside for the routing node
- The communication between Trusted Party (TP) and nodes is assumed secured
- Nodes are required to hash their unique identity to lessen storage overhead

Our protocol, TPAL aims at achieving the following goals:

- **Node authentication**: The receiver node which receives the message should be able to verify whether a received message is sent by the node who claimed to be the sender. Thus, the adversaries cannot pretend to be a legitimate node and inject counterfeit messages into the network without being detected
- **Message integrity**: The message receiver should be able to verify whether the message has been modified en-route by the adversaries or not
- **Intermediate node authentication**: Each forwarder node, on the routing path should be able to verify the authenticity of the message upon reception
- **Identity and location privacy**: The message sender's ID and location should not be known by the adversaries
- **Efficiency**: TPAL should be efficient in terms of computational and communication overhead

Our protocol, TPAL is an enhanced version of Martin protocol with a trusted party to help facilitate the authentication between nodes. TPAL uses ECC as it can provide the same security level of RSA while having a lower key size. The addition of pre-shared secret keys (K) prior to the distribution of nodes may remove the need to have another security layer for the 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 guided by the RPL in terms of nodes discovery thus can reduce unnecessary energy consumption. TPAL will also enhance the security mode option provided in RPL especially the Authenticated Mode (AM) which makes our protocol suitable to be deployed in the future to support the emerging technologies of IoT. We took the liberty in splitting our protocol architecture into two figures.

Figure 1 shows the architecture setup of TPAL protocol 1st phase, consist of a Trusted Party (TP) and several nodes. The nodes can request the security credential (public/private key) from a TP. TP is responsible for facilitating a key process if required to do so and authenticating nodes. TP also needs to monitor communication between nodes. Any heavy calculation will be handled by TP and nodes focus on authentication procedure. Each node that belongs to the same group in TP needs to communicate with TP before proceeding to the authentication procedure. Basically, this phase is mainly for the distribution of the public keys among the group nodes and the TP via a secure channel. This can eliminate any malicious nodes that try to insert itself into the network even though their keys do not belong in this setup.

Figure 2 shows the 2nd phase of TPAL architecture. This is a phase where it begins to authenticate between nodes, utilizing the security accreditations. Node A sends request authentication message to node B. Upon receiving this message, node B forwards that message and its own message to TP. After that, TP validates the messages by comparing the credentials provided by both nodes in the previous phase. Once validation is confirmed, node B proceeds the authentication with node A. Here, TP acts as a support party to help achieve authentication. Later, both nodes can proceed with mutual authentication with each other.

Table 2 highlights the notation for the protocol descriptions. Node A gets its credentials from TP and will run a mutual authentication with node B. In phase 1, each node needs to register themselves at TP as shown in Fig. 1. Each legal node will have their own key before been deployed. Later, they may use this key to request a valid credential from TP and thus register themselves in that TP group. However, TP will check if that node really belongs to the group by comparing the ID with TP's database. Any node whose hashed ID is not in the pre-stored ID table will be considered as an illegal node. Then only can TP generate public/private keys for each legal node.

DOI: 10.3844/jcssp.2018.1401.1411

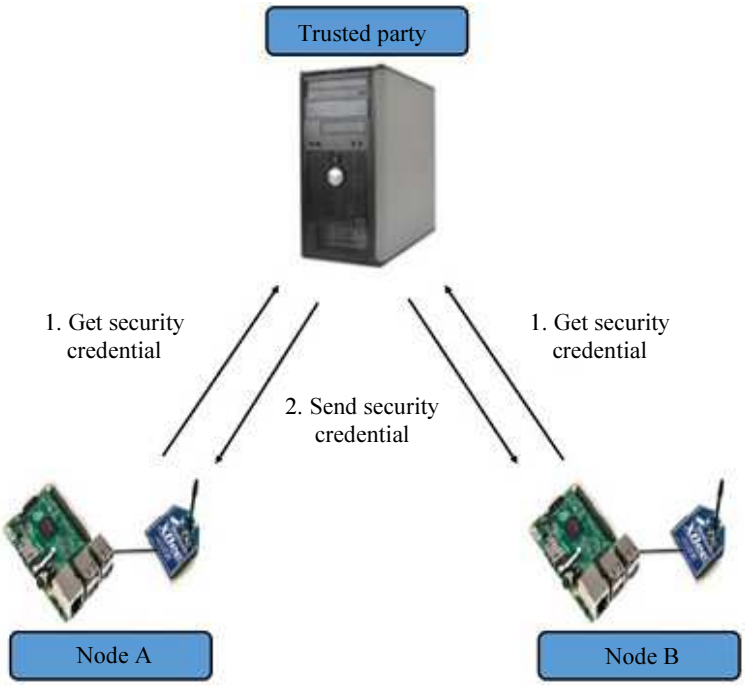

Fig. 1: TPAL architecture 1st phase

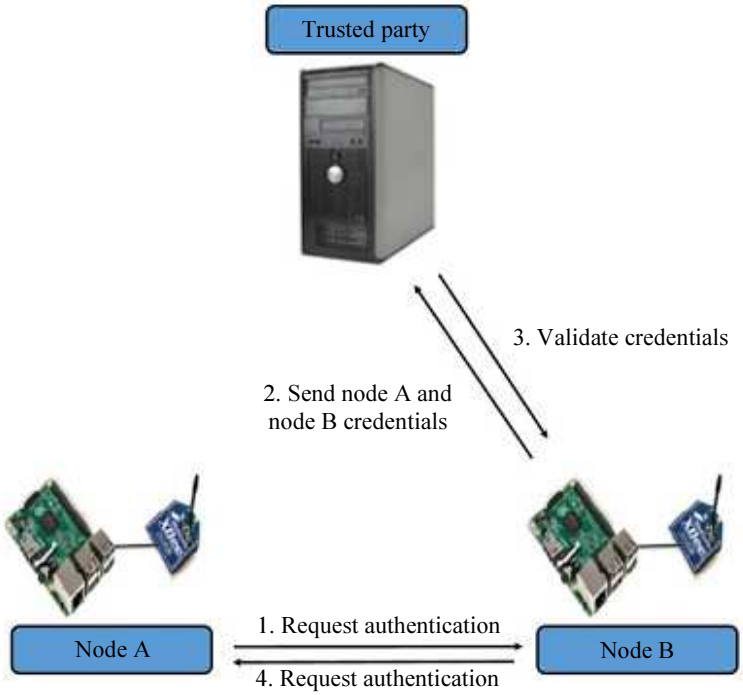

Fig. 2: TPAL architecture 2nd Phase

Figure 3 shows an approach used by TP to distribute the keys for each known hashed ID's nodes in the 1st Phase. TP may send a hashed message of the pre-shared key with its public key that belongs to TP and the node which TP communicates with and TP's public key as in Step 1. That node then replies with its hashed message and signed message that holds a TP's ID and both public keys as in Step 2. In Step 3, only then can, TP reply with a signed message containing a new key for that node.

In both initial message sequences as shown in Step 1 and Step 2 in Fig. 1, each participant needs to compare the received hashed message and public key, with their hash value of the pre-shared key and public key. Basically, if *H(K, Xtp)* from TP is equal with *H(K, Xtp)* in node then continue to communicate. Otherwise, they drop the communication if the information does not tally with what they have at that time.

Table 2: Notations used throughout the paper

Message	Meaning
A, B…	Name of nodes
TP	Trusted Party
E[m]	Encrypt message m
K	Pre-shared key
H[A]	Hashing value of node A
SigA, SigB	Signature of node A, node B
A → B:m	Message m sent to node B by node A

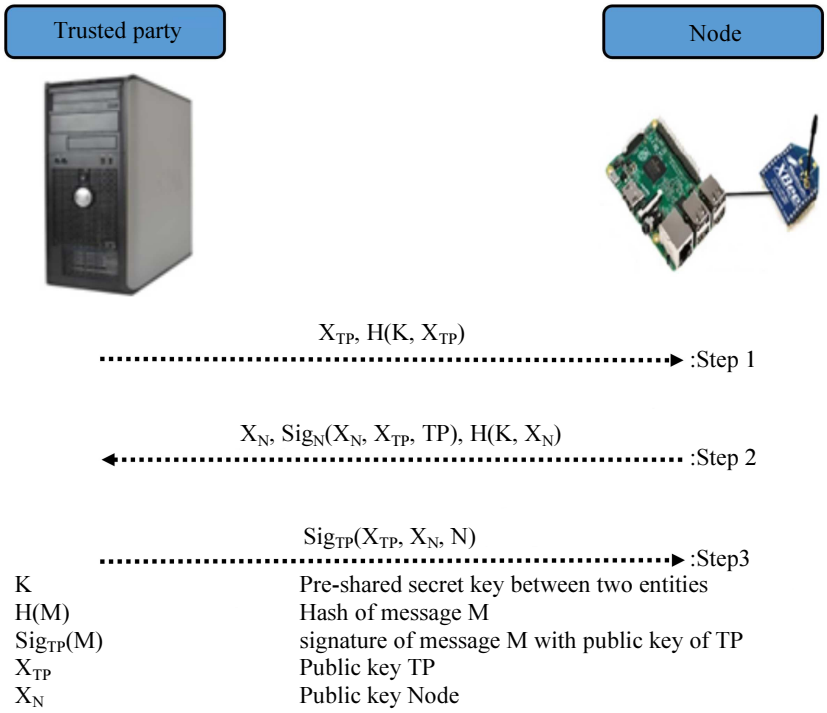

Fig. 3: Authentication steps between Node and TP (1st Phase) (Noack, 2014)

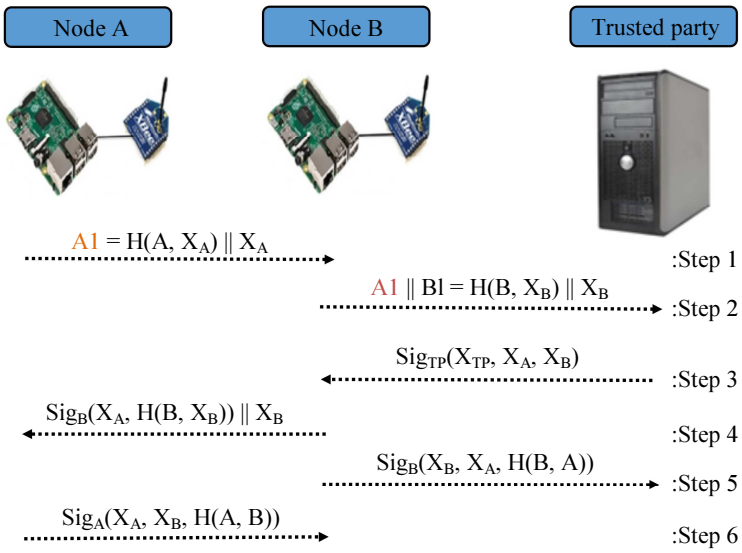

Fig. 4: Authentication steps between Nodes with help from TP (2nd Phase)

Figure 4 shows the protocol steps for the TPAL's 2nd Phase. In this phase, TP will act as a verifier of node authentications. Node A sends a message that contains the hash value of its pre-shared key combine with A's public key to node B in Step 1. Node B forwards the message from A to TP with B's hash message and its public key too as in Step 2. Once received by TP, it checks both messages by comparing their public key and hashed message with TP database. TP may acknowledge both nodes really belong to TP's group if only the comparison is successful.

In Step 3, TP then sends a signed message which contains both nodes public keys and its own public key to node B. This is to inform node B that node A is really who it claims to be and the one to attempt the authentication. If the comparison is not successful, TP will disregard that message. Upon not receive anything from TP for a while, node B will drop the authentication procedure.

In Step 4, if node B gets a reply from TP, node B then continues to send a message to node A which contains its signed hash ID and public key with node A's public key. Node B also sends a signed message to TP which contains both nodes' public keys and the hash value of its ID and node A's ID as shown in Step 5. For the final Step 6, if node A replies with a signed message containing the same message of what node B sends to TP, then authentication can be considered successful. Only then both A and B are authenticated to each other.

Analysis and Discussion

This section presents the security analyses of our proposed protocol, TPAL. To perform the analysis, Automated Validation of Internet Security Protocols and Applications (SPAN-AVISPA), a state-of-the-art push button tool for the automated security validation, is used to check whether the proposed protocol is vulnerable to attack specified by the protocol or not.

AVISPA is an automated tool used for formal verification, which provides functions for specification, verification, analysis, presentation and derivation of protocols and applications (Vigano, 2006). The High-Level Protocol Specification Language (HLPSL) is used by AVISPA in order to model a protocol. AVISPA converts the protocol specification written in HLPSL into Intermediate Format (IF) through HLPSL2IF.

Figure 5 presents the operational architecture of AVISPA. Currently, AVISPA supports four sub-modules, namely, On-the-Fly Model-Checker (OFMC: uses lazy intruder technique for state space models and incorporates symbolic technique to model Dolev-Yao intruder), Constraint-Logic-based Attack Searcher (CL-AtSe: Uses various optimization technique to reduce redundancies and uselessness in the protocol), SAT-based Model-Checker (SATMC: Works for typed protocol model) and Automatic Approximations for the Analysis of Security Protocols (TA4SP: Used for the unbounded verification of security properties of the protocol).

The TPAL protocol is divided into two parts, each of them is modeled in CAS+ before being converted in HLPSL and verified through AVISPA. The simulated flows of the two modeled steps are shown in Fig. 6 and 7. Basically, Fig. 6 shows an MSC flow for 1st Phase in TPAL mentioned in Fig. 3 while Fig. 7 shows the MSC flows for the 2nd Phase mentioned in Fig. 4.

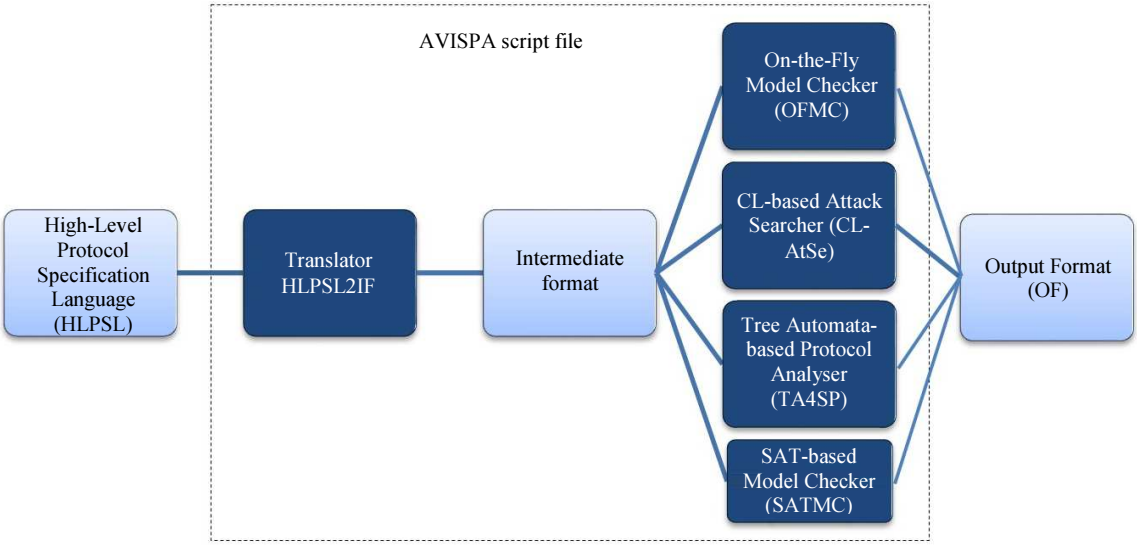

Fig. 5: The architecture of AVISPA

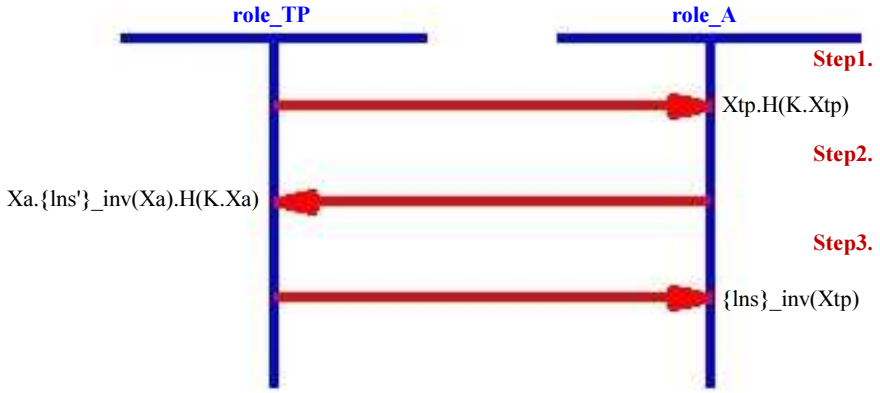

Fig. 6: MSC flow during 1st Phase which involve TP and Node

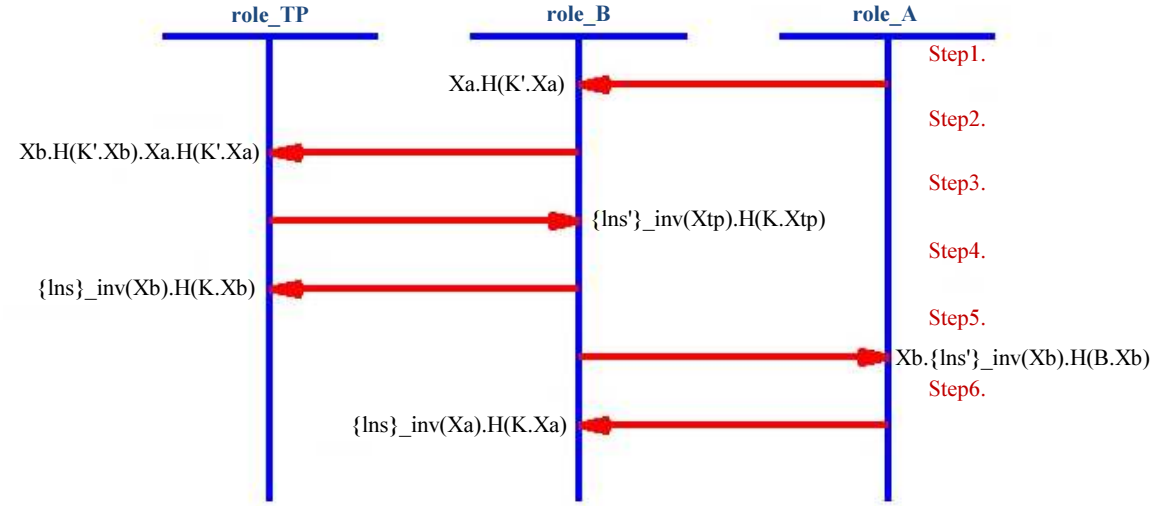

Fig. 7: MSC flow during 2nd Phase involves TP and Nodes

To test our protocol using AVISPA, we specify an environment for an intruder to attack our protocol based on the security property. In our case, an intruder has its own key, the knowledge of TP, Node B and Node A while acting as Node B. On the other hand, our specifications for this protocol contains 3 roles known as *role_TP*, *role_B* and *role_A*.

For the specification of roles, we identified and used one security goal and analyzed the protocol against this specified goal. The goal section is specified as below:

- *Authentication on TP_A_na; (1st Phase)*
- *Authentication on A_B_na; (2nd Phase*)

This goal is related to authentication as our protocol focused on node authentication. The “authentication_on TP_A_na” is for authentication of A by TP while the second goal “authentication_on A_B_na” is related to authentication of B by A.

As stated earlier, we have analyzed our protocol using OFMC and CL-AtSe model analyzers for analysis of our protocol. These two models are the most used in AVISPA (Genet, 2015; Ziauddin and Martin, 2013).

Figure 8 and 9 demonstrated the OFMC and CL-AtSe results for the Fig. 6 which is the 1st Phase of TPAL protocol.

1st Phase in our protocol is declared safe by both OFMC and CL-AtSe based on the given environment of the intruder. Here, CL-AtSe is much faster as compared to OFMC.

Figure 10 and 11 shown those of Fig. 7 step which is the 2nd Phase of TPAL.

Both backends show a safe result for the 2nd Phase of TPAL. As we can see, CL-AtSe is faster than OFMC. Basically, these results correspond to the initial analysis in our previous paper (Razali *et al*., 2018) and prove that the proposed TPAL protocol is safe from man-in-the-middle-attack.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 11 nodes
  depth: 5 plies
```

Fig. 8: The resulting output of OFMC for 1st Phase

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

Analysed: 4 states
Reachable: 2 states
Translation: 0.00 seconds
Computation: 0.00 seconds
```

Fig. 9: The resulting output of CL-AtSe for 1st Phase

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.03s
  visitedNodes: 10 nodes
  depth: 7 plies
```

Fig. 10: The resulting output of OFMC for 2nd Phase

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

Analysed: 13 states
Reachable: 6 states
Translation: 0.01 seconds
Computation: 0.00 seconds
```

Fig. 11: The resulting output of CL-AtSe for 2nd Phase

In addition, the higher the level of security, the more likely for the program to have a lower efficiency in terms of program execution such as 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 a low message and communication complexity.

In TPAL protocol, we assume that cryptographic hash (H) and asymmetric encryption or decryption processes have same message complexity of $E[m]$ where m is the size of the message and E is a cryptography process while X in $X[m]$ is for XOR process. Meanwhile, the unicast message (UC) requires $2E$ ($E[m]$ multiply by 2) operations for both encrypt and decrypt while broadcast message (BC) requires $[N+1]E$ (N is a reply message by the receiver). Both unicast and broadcast message is to determine the total communication complexity. From the whole execution of the protocol, the message complexity is determined by a total of each process occur in that particular protocol as shown in Table 3.

It can be seen that the message complexity of TPAL in both registration and authentication is slightly expensive compared to AKMS (Qin *et al*., 2016) but outperforms both Lu *et al*. (2016) and Farash *et al*. (2016). AKMS is less expensive in the message complexity than TPAL because AKMS is based on symmetric encryption scheme utilizing Delgado-Mohatar *et al*. (2011) approach with different key scheme while TPAL is based on asymmetric encryption.

It is probable that, thanks to the symmetric cryptography which requires lesser operation process but do not provide sufficient security level against keys protection. Even though TPAL is less efficient in term of message communication than AKMS, TPAL provides better security level of key protection and key management. TPAL also does not require the use of time synchronization between the trusted party and nodes as compared to scheme (Quan *et al*., 2015).

Table 3: Node processes involving message operation with different protocols

Protocol	Phase	Message complexity	Complexity time	Comm synch
TPAL	Registration	4*E*,2*H*	3*UC*	-
	Authentication	8*E*,4*H*	6*UC*	-
AKMS	Registration	(2+*N*)*E*,1*H*	1*BC*	-
	Authentication	4*E*,3*H*	3*UC*	-
Lu *et al*. (2016)	Registration	4*E*,10*H*,2*X*	2*UC*	-
	Authentication	8*E*,17*H*,15*X*	4*UC*	3*T*
Farash *et al*. (2016)	Registration	4*E*,6*H*,2*X*	2*UC*	2*T*
	Authentication	30*H*,16*X*	4*UC*	4*T*

Conclusion

We proposed a lightweight authentication protocol, TPAL, using public key encryption validated with SPAN-AVISPA. ECC is used here as it is a lightweight public key encryption that provides a shorter key length with the same level of security protection as RSA. A trusted party is introduced to handle heavy security operations and provide keys distribution, thus further moving heavy operations away from constrained nodes. By adopting ECC with pre-shared keys, we can validate the identity of the node. Furthermore, nodes only need to store other node ID's hash value and thus reduce the storage consumption. In addition, the authentication is guided by the routing protocol in terms of node discovery during routing path discovery. Thus, nodes that do not involve in the data transfer may not need to authenticate itself with every one of its neighbors and hence reduce energy consumption.

In the future, we are planning to put some mechanism to prevent an attack such as a replay attack after the authentication been performed without compromise TPAL's performance. Besides, we want to introduce TP with a blockchain technology to prevent TP from being harmed if it receives large requests. We also plan to reduce the message overhead in TPAL so that it can achieve better efficiency and implementing TPAL in RPL. We believed that TPAL can be a solution to the Authenticated Mode in RPL.

Acknowledgment

We would like to express our gratitude to the fellow researchers of the College of Computer Science and Information Technology (CSIT), UNITEN for their educational support.

Funding Information

This work was supported by the Ministry of Higher Education (MOHE) under the Fundamental Research Grant Scheme (FRGS).

Author's Contributions

Mohamad Faiz Razali: Offered writing support with all might.

Mohd Ezanee Rusli: Provided constructive supervision and intellectual commitment needed to finish writing this paper.

Norziana Jamil: Offered valuable advice and support in doing the analysis section.

Salman Yussof: Provided English language check, proofreading and insight in doing the introduction and conclusion section.

Ethics

This paper is original and it is not considered for publication somewhere else. The corresponding author has affirmed that all authors have read and approved the manuscript and thus no ethical issues may emerge after the publication of this manuscript.

References

Bala, D.Q., S. Maity and S.K. Jena, 2017. Mutual authentication for IoT smart environment using certificate-less public key cryptography. Proceedings of the 3rd International Conference on Sensing, Signal Processing and Security, May 4-5, IEEE Xplore Presss, Chennai, India, pp: 29-34. DOI: 10.1109/SSPS.2017.8071559

Banerjee, P., T. Chatterjee and S. Dasbit, 2015. LoENA: Low-overhead encryption based node authentication in WSN. Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Aug. 10-13, IEEE Xplore Press, Kochi, India, pp: 2126-2132. DOI: 10.1109/ICACCI.2015.7275931

Boyle, D. and T. Newe, 2008. Securing wireless sensor networks: Security architectures. J. Netw., 3: 65-77. DOI: 10.4304/jnw.3.1.65-77

Brandt, A., J. Hui, R. Kelsey, P. Levis and K. Pister *et al*., 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Internet Engineering Task Force (IETF).

Chang, Q., Y. Zhang and L. Qin, 2010. A node authentication protocol based on ECC in WSN. Proceedings of the International Conference on Computer Design and Applications, Jin. 25-27, IEEE Xplore Press, Qinhuangdao, China, pp: V2-606-V2-609. DOI: 10.1109/ICCDA.2010.5541288

Delgado-Mohatar, O., A. Fúster-Sabater and J.M. Sierra, 2011. A light-weight authentication scheme for wireless sensor networks. Ad Hoc Netw., 9: 727-735. DOI: 10.1016/j.adhoc.2010.08.020

Dhillon, P.K. and S. Kalra, 2017. A lightweight biometrics based remote user authentication scheme for IoT services. J. Inform. Security Applic., 34: 255-270. DOI: 10.1016/j.jisa.2017.01.003

Farash, M.S., M. Turkanović, S. Kumari and M. Hölbl, 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Netw., 36: 152-176. DOI: 10.1016/J.ADHOC.2015.05.014

Genet, T., 2015. A short SPAN + AVISPA tutorial.

Guicheng, S. and Y. Zhen, 2013. Application of elliptic curve cryptography in node authentication of internet of things. Proceedings of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Oct. 16-18, IEEE Xplore Press, Beijing, China, pp: 452-455. DOI: 10.1109/IIH-MSP.2013.118

Hammi, M., E. Livolant, P. Bellot, A. Serhrouchni and M. Hammi *et al*., 2017 A lightweight mutual authentication protocol for the IoT. Proceedings of the iCatse International Conference on Mobile and Wireless Technology, (MWT' 17), Kuala Lumpur, Thailand, pp: 1-10. DOI: 10.1007/978-981-10-5281-1

Jiang, Q., J. Ma, F. Wei, Y. Tian, J. Shen and Y. Yang, 2016. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. J. Netw. Comput. Applic., 76: 37-48. DOI: 10.1016/j.jnca.2016.10.001

Li, N., D. Liu and S. Nepal, 2017a. Lightweight mutual authentication for IoT and its applications. IEEE Trans. Sustainable Comput., 2: 359-370. DOI: 10.1109/TSUSC.2017.2716953

Li, X., J. Niu, M.Z.A. Bhuiyan, F. Wu and M. Karuppiah *et al*., 2017b. A robust ECC based provable secure authentication protocol with privacy protection for industrial internet of things. IEEE Trans. Indus. Inform., 3203: 1-11. DOI: 10.1109/TII.2017.2773666

Liu, Y. and Y. Yan, 2012. A lightweight and scalable key management scheme for heterogeneous sensor networks. Proceedings of the 5th International Conference on BioMedical Engineering and Informatics, Oct. 16-18, IEEE Xplore Press, Chongqing, China, pp: 1393-1397. DOI: 10.1109/BMEI.2012.6513216

Lu, Y., L. Li, H. Peng and Y. Yang, 2016. An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks. Sensors, 16: 837. DOI: 10.3390/s16060837

Noack, M., 2014. Optimization of two-way authentication protocol in internet of things. University of Zurich.

Porambage, P., C. Schmitt, P. Kumar, A. Gurtov and M. Ylianttila, 2014. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. Proceedings of the IEEE Wireless Communications and Networking Conference, Apr. 6-9, IEEE Xplore Press, Istanbul, Turkey, pp: 2728-2733. DOI: 10.1109/WCNC.2014.6952860

Qin, D., S. Jia, S. Yang, E. Wang and Q. Ding, 2016. A lightweight authentication and key management scheme for wireless sensor networks. J. Sensors, 2016: 1-9. DOI: 10.1155/2016/1547963

Quan, Z., T. Chunming, Z., Xianghan and R. Chunming, 2015. A secure user authentication protocol for sensor network in data capturing. J. Cloud Comput., 4: 6-6. DOI: 10.1186/s13677-015-0030-z

Razali, M.F., M.E. Rusli, N. Jamil, R., Ismail and S. Yussof, 2017. The authentication techniques for enhancing the Rpl security mode: A survey. Proceedings of the 6th International Conference on Computing and Informatics, Apr. 25-27, Universiti Utara Malaysia, Kuala Lumpur, pp: 735-743.

Razali, M.F., M.E. Rusli, N. Jamil and S. Yussof, 2018. Two phases authentication level (tpal) protocol for nodes authentication in internet of things. J. Fundamental Applied Sci., 10: 190-200. DOI: 10.4314/jfas.v10i2s.16

Rghioui, A., R. Abdmeziem, S. Bouchkaren and M. Bouhorma, 2015. Symmetric cryptography keys management for 6lowpan networks. J. Theoretical Applied Inform. Technol., 73: 336-345.

Saleh, M., N. El-meniawy and E. Sourour, 2015. Authentication in flat wireless sensor networks with mobile nodes. Proceedings of the IEEE 12th International Conference on Networking, Sensing and Control, Apr. 9-11, IEEE Xplore Press, Taipei, Taiwan, pp: 208-212. DOI: 10.1109/ICNSC.2015.7116036

Santoso, F.K. and N.C.H. Vun, 2015. Securing IoT for smart home system. Proceedings of the International Symposium on Consumer Electronics, Jun. 24-26, IEEE Xplore Press, Madrid, Spain, pp: 1-2. DOI: 10.1109/ISCE.2015.7177843

Shen, J., S. Chang, J. Shen, Q. Liu and X. Sun, 2018. A lightweight multi-layer authentication protocol for wireless body area networks. Future Generat. Comput. Syst., 78: 956-963. DOI: 10.1016/j.future.2016.11.033

Shivraj, V.L., M.A. Rajan, M., Singh and P. Balamuralidhar, 2015. One time password authentication scheme based on elliptic curves for Internet of Things (IoT). Proceedings of the 5th National Symposium on Information Technology: Towards New Smart World, Feb. 17-19, IEEE Xplore Press, Riyadh, Saudi Arabia, pp: 1-6. DOI: 10.1109/NSITNSW.2015.7176384

Vigano, L., 2006. Automated security protocol analysis with the AVISPA tool. Electr. Notes Theor. Comput. Sci., 155: 61-86. DOI: 10.1016/j.entcs.2005.11.052

Ziauddin, S. and B. Martin, 2013. Formal analysis of ISO/IEC 9798-2 authentication standard using AVISPA. Proceedings of the 8th Asia Joint Conference on Information Security, Jul. 25-26, IEEE Xplore Press, Seoul, South Korea, pp: 108-114. DOI: 10.1109/ASIAJCIS.2013.25