How to cite this paper:

Mohamad Faiz Razali, Mohd Ezanee Rusli, Norziana Jamil, Roslan Ismail, & Salman Yussof. (2017). The authentication techniques for enhancing the RPL security mode: A survey in Zulikha, J. & N. H. Zakaria (Eds.), Proceedings of the 6th International Conference on Computing & Informatics (pp 735-743). Sintok: School of Computing.

# THE AUTHENTICATION TECHNIQUES FOR ENHANCING THE RPL SECURITY MODE: A SURVEY

**Mohamad Faiz Razali, Mohd Ezanee Rusli, Norziana Jamil, Roslan Ismail, Salman Yussof**

*College of Computer Science and Information Technology,*
*Universiti Tenaga Nasional, Malaysia,*
*techfree91@gmail.com,{Ezanee, Norziana, Roslan, Salman}@uniten.edu.my*

**ABSTRACT**. The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) was introduced as the routing standard for the Internet of Things (IoT) by the Internet Engineering Task Force (IETF) in 6LowPAN environment networks. It supports a secure version of routing control messages while providing three security support modes known as Unsecured, Pre-installed and Authenticated Mode. Unsecured Mode is a default usage mode of RPL which is currently used for exchanging routing message. For now, RPL uses AES/CCM in order to provide confidentiality and integrity in its specification. Authenticated Mode is reserved for future work and must not be supported by symmetric cryptography for nodes intending to be a router in RPL network. The outside device needs to be authenticated to join the RPL network as a router. Currently, the RPL specification in RFC 6550 does not state how asymmetric cryptography can be implemented if the device is to be authenticated and to operate as a router. This paper provides a survey of lightweight authentication schemes proposed for LLN.

**Keywords**: RPL, security mode, authentication, cryptography, lightweight

## INTRODUCTION

As the Internet keeps growing and computer networks become much bigger each day, security becomes one of the most important pillars and a critical aspect to be considered. The same situation happens to Internet of Things (IoT). It is estimated that the number of IoT-enabled devices will reach approximately 25 billion by year 2025 ("Gartner Says 4.9 Billion," 2014). With the contribution of the Internet, IoT becomes an emerging technology enabling other technologies to be combined such as radio frequency identification (RFID) technology, wireless communication technology and electronic product code (EPC) standard.

Within IoT, all things in this world may become translucent due to the consistency of global real time information sharing. This is a reason why security becomes more sensitive within the development of IoT. Cyber-attackers are waiting for any opportunity available and any chances visible in IoT to hack into the network thus jeopardizing the entire network (Wen, Dong, & Zhang, 2012). Network nodes interact with each other using wireless channels. These nodes may be left unattended as human workers cannot possibly attend to all of them. This situation could make them vulnerable to security and network attacks. Cyber-attackers can hijack the communication by providing their own nodes into the network. Furthermore, they can try to eavesdrop on messages exchanged between legal nodes and thus

modify the contents. Moreover, attackers can also try to prevent messages from reaching their target destination. In some situations, they may try to execute Denial of Service (DOS) attacks to disrupt the network services.

Besides, the emergence of IoT from the Internet combined with real world smart objects has resulted in the large scale deployment of Low power and Lossy Networks (LLN). An example of LLN is Wireless Sensor Networks which is typically resource constrained in terms of memory, power resource and computational capability and often prone to encounter high loss rate in communication. In order to address this kind of network, Internet Engineering Task Force (IETF) working group has proposed a protocol known as Routing Protocol for Low power and Lossy Networks (RPL) at the routing layer (Ed, et al., 2012). RPL also has security support mode for security purposes especially for new nodes to join a network. Nevertheless, due to the constrained nature of RPL based networks and the complexity of RPL itself, the security modes are usually optional.

Cryptography mechanisms are used as a shield for authentication purposes to hide the information thus often making it difficult to be read by unauthorized parties. The operation usually involves encryption and hashing. For now, RPL uses symmetric encryption known as AES/CCM in their specification (Tsao, et al., 2015). But as cyber-attackers are always one step ahead, they could find a way to enter the network since symmetric encryption uses the concept of the same secret key to be exchanged between nodes. To read encrypted data, we must have a key to enable us to decrypt it. However, if the nodes are compromised in this case, such as the nodes are captured or the keys have become known to the attackers, cryptography can no longer safeguard the network.

For LLN networks, due to the nature of its constraints, symmetric cryptography is the common choice to be proposed (David & Thomas, 2008). There are also some key predistribution schemes mentioned in the paper (Saleh & Sourour, 2015). In an extreme situation, all nodes share the same secret key, which makes key management much easier to handle. Unfortunately, this scheme is very much vulnerable since the disclosure of the keys would affect the whole network. If the cyber-attackers gain access to the key in this kind of network, they could enter or disguise to be a node using that particular key and gain information within them, which ultimately jeopardize the network. At one side, each pair of nodes shared a distinct key. Thus, if a key is disclosed, only two nodes are compromised. This is a viable option to tackle the problem of same secret key for all nodes. However, carrying a large number of pre-distribution keys will only make the node use a large portion of memory storage. Thus, it makes the expandability in LLN to be very limited.

Due to the constrained environment of this kind of network, and the possibility of any malicious attackers to inject false data, the authentication scheme especially in RPL must be improved. This paper aims to give a general insight on how RPL security mode is defined and provide a brief description on a number of protocols proposed by other researchers focusing on the node authentication which may help in improving security.

The rest of the paper is organized as follows. The following section explains the authentication concept and RPL as a protocol including its security modes and the security issues involving RPL. Next, the authentication schemes based on encryption techniques from various researchers which could be applied into RPL will be discussed. Finally, a conclusion is presented.

## RPL: CONCEPT OF AUTHENTICATION AND RPL SECURITY MODES

### Authentication

Authentication is used in order to ensure the identity of a claimant is what he/she/it claims to be and also a critical part of network security scheme. In other word, authentication is actually a mechanism to prove if he or she or something is indeed who or what it claims to be. Authentication can be performed one way or two ways depending on the situation (Saleh & Sourour, 2015). In a two ways authentication, both parties involved need to prove their identities towards each other. However authentication just identifies who the person or system claim to be but does not determine what kind of tasks a claimant can do ("Understanding Authentication," 2016). Many authentication schemes exist to this day and all of them serve the mutual goal which is to ensure the user identity is correct. To date, there are several authentication schemes that have been designed for computer networks but some were discovered later to be flawed (David & Thomas, 2008).

In terms of IoT, authentication is basically the first step that occurs when a node is connecting to a new network. Many different authentication schemes exist in IoT network. One scenario that highlights the importance of authentication is in a smart home network. In this example, any new devices such as smartphones from visitors that request to join the network need to be authenticated in order to avoid malicious intruders from gaining access to the network.

In order to setup a security mechanism of a network, the characteristics and requirements of the networks have to be observed. For example, there are different characteristics between a network of a smart home alarm security system and a tsunami alarm system. For smart home network, the power consumption is not a major issue since the owner can change the depleted battery quite easily. Therefore, s/he can opt to adopt high and complex security mechanism. On the contrary, the administrator of a tsunami alarm system has to consider a mechanism that is less complex and has lower power consumption due to the fact that the coverage area is wide and not easily accessible. Therefore, a security mechanism that is energy efficient is preferred for IoT network.

### RPL Concept and Security Modes

RPL has been introduced by IETF group since 2012. It is designed to be an efficient routing protocol for LLN environment. In other word, RPL provides solution for energy constrained devices which is a critical characteristic for LLN as RPL ensures reduction in the overall power consumption by minimizing the control traffic. RPL is also able to sustain a variety of divergent link layers such as ones that are constrained, potentially lossy or typically utilized in conjunction with host or router devices with very limited resources. An example is in urban applications where the nodes will be placed outdoors in urban environments to improve people's living conditions or to monitor law compliance. Moreover, RPL has the ability to quickly build up network routes, to disperse routing knowledge among nodes and to adapt to the topology in a very efficient way.

Because RPL nodes need to exchange information between each other especially during reconstruction of RPL topology, they should implement a mechanism to authenticate the exchanged messages. RPL has various routing control messages such as DIO, DIS, and DAO-ACK. These control messages includes messages that are relevant only in networks with security enabled. A component of code field in RPL message will identify whether the RPL message is secure or not. Basically, RPL also defines three security modes for these control messages as shown in here:

- *Unsecured Mode*: RPL control messages are sent without any additional security mechanism. It could be using other present security primitives such as link-layer security to meet application security requirements.
- *Pre-installed Mode*: Nodes joining a RPL Instance either as a host or a router using preinstalled symmetric keys while providing message confidentiality, integrity and authenticity.
- *Authenticated Mode* (AM): Nodes have preinstalled keys as in preinstalled mode, but the key can only be used to join a RPL Instance as a host. However, to join as a router requires obtaining a different key from a key authority which is responsible for authenticating and authorizing the device for this purpose.

Unsecured mode is the default usage mode of RPL. In this mode, no security is applied to routing control messages. Currently, AES with CCM mode (Counter with CBC-MAC) is adopted in order to support security in RPL. The AES will encrypt the RPL ICMPv6 message after the security section inside the RPL control message until the last part of the packet. The CCM will be added to AES in order to provide authentication and confidentiality. In Pre-installed Mode, the nodes will be using preinstalled symmetric key to provide security for the exchanged messages either as a host or as a router. But for the router which may have crucial information about the network, it could later succumb to the cyber-attacker if the preinstalled key becomes known to them. AES could provide the security needed for now but since it is a symmetric encryption, a more secure encryption that is based on asymmetric technique is recommended.

As for the Authenticated Mode, it is actually a reserve mode for future work. This mode will be used for a node intending to be a router. At the moment, the RPL specification defines that AM must not be supported by symmetric cryptography. However, it does not state how asymmetric cryptography could be employed in order to support node authentication and a key retrieval by the node intending to operate as a router. One of the issues with asymmetric cryptography relates to its expensive computation. Hence, lightweight encryption for RPL authentication scheme is needed. Furthermore, IETF working group has also announced a call for help to make a better RPL in terms of its node authentication.

These basic security features of RPL may protect the network against external attack as reported in Tsao et al. (2015). Nevertheless, by capturing a node and extracting security information, cyber attackers can gain access into the network and modify the routing topology. Thus, a strong node authentication is required in order to defend against this kind of attack. Unfortunately, due to the characteristics of resource constrained nodes, such mechanisms are currently limited.

Mayzaud et al. (2016) in their paper, have established a taxonomy of the attacks against RPL protocol, by grouping them into three main categories including attacks targeting network resources, attacks modifying the network topology and attacks related to network traffic with the assumption that the keys have been compromised. In their case, the cyber-attackers have already gained the secret keys thus the authentication could no longer protect the network. They also make a comparison of the attack's properties and discuss existing countermeasures. Tsao et al. have provided the threat analyses on possible RPL security issues according to regular security pillars such as confidentiality, integrity, availability and authentication. They also included recommendation and guidelines on how to counteract these issues but does not specify how the attacks are stimulated on RPL.

In order to make RPL to withstand incoming attack from cyber-attackers either from the outside or the inside and to be more secure, there is a need to enhance RPL especially for its

Authenticated Mode. There is also another problem related to the key management due to the fact that this mode requires a different key retrieval from another key authority. The key must be negotiated and periodically refreshed to provide long term and effective security. Thus, a lightweight key management mechanism is also required.

## AUTHENTICATION SCHEMES

Table 1 highlights authentication schemes that have been proposed by other researchers.

**Table 1. Lightweight Authentication Schemes**

| Researchers | Encryption Type | Technique | Details | RPL Security Mode Applicability |
|---|---|---|---|---|
| Chang, Zhang, and Qin (2010) | Asymmetric | The authentication method is based on XKAS Key Agreement Scheme while adopted ECC. | This scheme improved a node authentication stage by enhancing the previous Identity Authentication System published in 2007. The node only stores the unique identity hash value thus reduce the consumption of the storage. | Authenticated Mode |
| Liu and Yan (2013) | Symmetric | It is based on Exclusion Basis System and keyed-hash functions (HMAC) | The scheme provides periodic or on demand key refreshment with node authentication | Pre-installed Mode |
| Porambage et all (2014) | Symmetric and asymmetric | It is based on AES and ECC | This scheme requires cryptography credentials to the edge devices and end users, and thus authenticating mutual communication. | Pre-installed Mode |
| Guicheng and Zhen (2014) | Asymmetric | It is based on ECC | Both RFID authentication and node authentication used implementation of ECC. | Authenticated Mode |
| Shivraj, A, Singh, and P (2015) | Asymmetric | Modifying of lightweight Identity Based Elliptic Curve Cryptography scheme into Lamport's OTP algorithm. | With the same security level provided, the scheme performs on par with the existing One Time Password with advantages of a smaller key size. | Authenticated Mode |
| Santoso and Vun (2015) | Symmetric and asymmetric | This scheme uses 2 rounds of authentication and the encryption is based on ECC and Elliptic Curve Diffie-Hellman | User needs to load the IoT's device credential into the mobile device. Later the details will be inserted into gateway using the same method. | Authenticated Mode |
| Rghioui, Abdmeziem, Bouchkaren, and Bouhorma (2015) | Symmetric | It is based on the use of a remote server for authentication and security keys management for 6LowPAN networks | A hybrid key management scheme which depends on the control of a Remote Server and also based on the internal device key generation to avoid sharing keys in the network | Pre-installed Mode |
| Banerjee, Chatterjee, and DasBit (2015) | Symmetric | Light computationally operation, dynamic key generation | This scheme produced low overhead with energy efficient node authentication. | Pre-installed Mode |

| | | | | |
|---|---|---|---|---|
| Saleh and Sourour (2015) | Symmetric | This scheme allows nodes to discover common keys during routing path discovery. It is possible that no common key will be found between nodes. | The scheme is integrated with routing protocol especially SPIN thus eliminated unnecessary protocol execution. | Pre-installed Mode |

Chang et al. (2010) proposed an improved version of authentication protocol which is based on Elliptic Curve Cryptography (ECC). The scheme uses 'Identity Authentication System based on ECC' as their basis. The scheme can be used in Wireless Sensor Network (WSN). They enhanced the authentication phase of the nodes by implementing the XKAS Key Agreement Scheme. This scheme could be implemented into RPL due to the asymmetric cryptography used inside it in order to tackle the Authenticated Mode problem mentioned before this, besides giving better security for node intended to be a router in RPL networks to be authenticated.

Saleh and Sourour (2015) proposed a node authentication protocol that enables nodes to be authenticated during the routing process and use symmetric cryptography. The authentication is guided by the routing process thus eliminating any excessive unnecessary protocol executions hence preventing any malicious nodes from joining themselves into data routes. Thus this scheme achieves two tasks at once while using less energy. This scheme has been integrated with TinyOS Beaconing and SPIN protocol simulation thus proved that it can be used in the routing protocol.

Banerjee et al. (2015) proposed a low overhead encryption in terms of node authentication. By using the light operations in each component of the algorithm, this scheme achieved lightweight. The scheme is divided into two parts involving a sender type algorithm and a receiver type algorithm. The sender side encrypts the 32-bit unique id (uid) of the sender node and generates a 20-bit encrypted uid with embedded key-hint sent to the receiver. The receiver side will run the same algorithms so that it can decypher the number. It later verifies the uid with the one stored in its neighbor list. If a match is found then the authentication process is successful.

Porambage et al. (2014) proposed an authentication between edge nodes and end users. It is a two phased authentication scheme in order to allow the edge nodes and end users to communicate in secure connections. This scheme is based on an ECC. It also has been made lightweight due to the use of implicit certificates for mutual authentication and also supporting heterogeneity of the nodes and end users.

Guicheng and Zhen (2014) proved that ECC is a reliable candidate to be used in node authentication compared to the RSA. They showed that an ECC with a key length of 162 bits shows the same security level as RSA with the key length of 1024 bits. Due to this, Guicheng believed that ECC can be implemented in RFID tags and also has proved that it is feasible to embed ECC into node authentication in IoT.

Shivraj et al. (2015) proposed One Time Password (OTP) scheme based on lightweight Identity Based Elliptic Curve Cryptography scheme (IBE) and Lamport's OTP algorithm. Due to the fact that hash based Lamport's OTP scheme is prone to attacks and others are computationally expensive, the authors replaced the hash function with the proposed function based on IBE scheme. The scheme does not depend on the previous keys thus used less memory resources and also does not store the keys. In their experiment, the scheme performs

on par with the existing OTP schemes with the difference of having a smaller key size and lesser infrastructure.

Santoso and Vun (2015) proposed an authentication scheme to be used in a smart home wifi system. AllJoyn framework is used as a base and the scheme also uses a gateway for authentication process. The ECC is used in the process and later, Elliptic Curve DiffieHellman will be used to create a shared key. But it is not very convenient as the user needs to enter the information required by hand each time. This scheme allows the user to configure the system through mobile devices.

Rghioui et al. (2015) proposed a security key management scheme for 6LoWPAN network. The scheme is a hybrid security solution based on symmetric and asymmetric encryption. The symmetric encryption uses less energy to compute and the asymmetric encryption provides end to end security establishment. Thus, this scheme maximizes the security performance with less resource consumption.

Liu and Yan (2013) presented a key management scheme for heterogeneous sensor networks. The scheme provides demand key refreshment periodically and node authentication. The keys are updated using keyed hash function to avoid data collision by compressing them into a fixed length. This scheme also makes nodes more resilient against node capture as each pair of nodes has a different shared pairwise key. The scheme is based on Exclusion Basis System (EBS) and simple symmetric primitives.

Based on the proposed schemes above, we observed that these schemes have beneficial to be applied for RPL security modes. Like a padlock, the concept is still the same as to provide better security even though there are many kinds of padlocks in the market place such as biometric padlock and key padlock. Each padlock has its own suitability for its customer's needs. The same goes to RPL, which now uses symmetric cryptography to provide authentication due to the resource constrained deployed nodes. There is a need for RPL to enhance its node authentication especially its Authenticated Mode which is now still in reserved state.

Based on the literature review conducted, we have established a taxonomy of authentication schemes from researchers which could help to enhance the RPL Security Mode especially in node authentication. The established taxonomy consists of symmetric, asymmetric and combinations of both. The taxonomy is depicted in Figure 1.

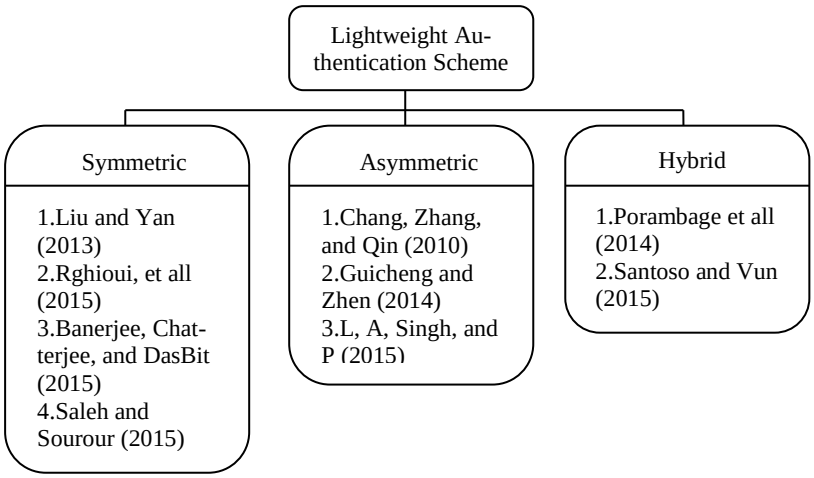


**Figure 1. A Taxonomy on Lightweight Authentication Schemes.**

## CONCLUSIONS

In this paper, we have conducted a survey on lightweight authentication schemes specifically for LLN. These schemes have the potential to be integrated into RPL to enhance RPL's security mechanism especially the Authentication mode. Based on this survey, a taxonomy of the lightweight authentication schemes has been presented. We believe that this paper may provide some grounds for future researchers in developing new solutions and perhaps improving RPL authentication security modes.

## ACKNOWLEDGMENTS

The authors would like to thank to the Ministry of Education for the funding of this research under the Fundamental Research Grant Scheme (FRGS) and fellow lecturers of College of Computer Science and Information Technology especially Dr. Mohd Ezanee Rusli for assistance.

## REFERENCES

Banerjee, P., Chatterjee, T., & DasBit, S. (2015). LoENA: Low-overhead Encryption based Node Authentication in WSN. *ICACCI*, 2126-2132.

Chang, Q., Zhang, Y.-p., & Qin, L.-l. (2010). A Node Authentication Protocol based on ECC in WSN. *ICCDA*, 606-609.

David, B., & Thomas, N. (2008). Securing Wireless Sensor Network: Ssecurity Architectures. *Journal of Networks*, 65-77.

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

*Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015*. (2014, November 11). Retrieved May 14, 2016, from Gartner Press Release: http://www.gartner.com/newsroom/id/2905717

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, 1294--1311.

Guicheng , S., & Zhen, Y. (2014). Application of Elliptic Curve Cryptography in Node Authentication of Internet of Things. *Intelligent Information Hiding and Multimedia Signal Processing*, 452-455.

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

Liu, Y., & Yan, Y. (2013). A Lightweight and Scalable Key Management Scheme for Heterogeneous Sensor Networks. *Biomedical Engineering and Informatics*, 1393-1397.

Mayzaud, A., Badonnel, R., & Chrisment, I. (2016). A Taxonomy of Attacks in RPL-based Internet of Things. *International Journal of Network Security, IJNS*, 459-473.

Perrey, H., Landsmann, M., Ugus, O., Schmidt, T. C., & Wählisch, M. (2013). TRAIL: Topology Authentication in RPL. *CoRR*.

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

Rghioui, A., Abdmeziem, R., Bouchkaren, S., & Bouhorma, M. (2015). Symmetric Cryptography Key Management for 6LowPAN Networks. *JATIT*, 336-345.

Saleh, M., & Sourour, E. (2015). Authentication in Flat Wireless Sensor Networks with Mobile Nodes. *IEEE 12th International Conference on Networking, Sensing and Control* (pp. 208-212). Taiwan: IEEE.

Santoso, F. K., & Vun, N. C. (2015). Securing IoT for Smart Home System. *International Symposium on Consumer Electronics*.

Stinson, D. R. (2005). *Cryptography: Theory and Practice, Third Edition.* Chapman and Hall/CRC.

Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., & Ed, R. M. (2015, January). *A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs).* Retrieved from Internet Engineering Task Force (IETF): http://www.ietf.org/rfc/rfc7416.txt

*Understanding Authentication, Authorization, and Encryption*. (n.d.). Retrieved August 12, 2016, from Boston University Information Services & Technology: https://www.bu.edu/tech/about/security-resources/bestpractice/auth/

Wen, Q., Dong, X., & Zhang, R. (2012). Application of Dynamic Variable Cipher Security Certificate in Internet of Things. *2nd International Conference on Cloud Computing and Intelligence Systems*, 1062-1066.