Securing the Internet of Things Devices Using Pre-Distributed Keys

El Hajjar, A.

Securing the Internet of Things Devices Using Pre-Distributed Keys

Ayman El Hajjar
Department of Computer Science
Birkbeck, University of London
Email: ayman@dcs.bbk.ac.uk
Supervised by Professor George Roussos Dept of Computer science
& Dr Maura Paterson Dept. of Economics, Mathematics and statistics

***Abstract*—The paper outlines the state of the art, problems and challenges in the Internet of things (IoT) security. It investigates how the key pre-distribution algorithm of Eschenauer and Giglor designed for Distributed Sensor Networks(DSN) performs when applied on the IoT for 6LoWPAN networks. A simulation that uses the Contiki Operating System was developed in order to explore the performance of the algorithm on those devices. After an explanation of the research methodology and the details of the experiment conducted, we present the results from the experiment in comparison with the results obtained by Eschenauer & Giglor.**

I. Introduction and Motivation

The Internet of Things refers to a world-wide network of interconnected heterogeneous objects (sensors, actuators, smart devices, smart objects, RFID, embedded computers and so on) uniquely addressable based on standard communication protocols [1]. In a common Wireless Sensor Network (WSN), each node plays an important role to ensure data confidentiality, integrity, availability and authentication. For those nodes to be attacked, it requires a physical presence near the targeted node in order to attack it. The Internet of Things interconnects WSN networks to the Internet and thus there is no need for location proximity and attacker would be able to attack any WSN node from the Internet.

For this reason, authentication between devices communicating in the IoT network became a necessity. This includes securing messages transmitted in the Routing Protocol for lossy Networks (RPL) as the security was not part of the protocol standard. Threats due to authentication failure is a main issue for motes joining the RPL Routing table as discussed in the IETF Routing Over Low Power and Lossy networks (ROLL) security threats draft [2]. A suggestion to use keys pre-distribution was made in the protocol draft. This suggestion did not specify which key pre-distribution protocol to use.

This paper suggests the use of the key-pre distribution algorithm proposed by Eschenauer & Giglor in the context of the IoT using 6LoWPAN adaption layer protocols.

II. Background to Research topic

6LoWPAN: Low Wireless Personal Area Networks are simple low cost communication networks that allow wireless connectivity in devices with limited power and relaxed throughput requirements. The 6LoWPAN adaptation layer concept originated from the idea that Internet Protocols could and should be applied even to the smallest devices, and that low-power devices with limited processing capabilities should be able to participate in the IoT [3]. Internet Protocol version 4 will not be able to accomodate the large number of LR-WPAN devices that is expected to be deployed in the IoT and thus IPv6 will be used for addressing of the IoT devcices. [4] Some are potentially left unattended or hard to reach and in harsh conditions. Any protocol used on those networks should take into consideration this unreliable nature of communication [5].

RPL: Routing in Low Power and Lossy networks (LLN) should be able to self manage and to self heal without requiring manual intervention. Routing Protocol for Low-Power and Lossy Networks (RPL)

is a distance vector IPv6 routing protocol designed for Low-Power and Lossy Networks (LLNs). RPL constructs a Directed Acyclic Graph (DAG) that attempts to minimize path costs to the DAG root according to a set of metrics and objective functions [5]. RPL draft includes two security modes, one called preinstalled, where motes joining an RPL instance have preinstalled keys that enable them to process and generate secured RPL message and another mode that is called authenticate. In authenticated mode motes have preinstalled keys as in preinstalled mode, but the preinstalled key may only be used to join a RPL instance as a leaf [6].

Keys Pre-Distribution for Distriuted Sensor Networs DSN: Traditional key exchange and key pre distribution protocols based on infrastructure using trusted third parties are impractical for large scale distributed sensor networks. A key management scheme for distributed sensor networks DSN proposed in [7] requires memory storage for only a few tens to a couple of hundred keys, and yet has similar security and superior operational properties when compared to those of the pair wise private key sharing scheme. This scheme relies on probabilistic key sharing among the motes and uses a simple shared key discovery protocol for key distribution. First and prior to DSN deployment, a ring of keys is distributed to each sensor mote, each key ring consisting of randomly chosen k keys from a large pool of P keys which is generated offline. Even if two motes do not share a key the pair of motes can use the path of an existing pair wise path to exchange keys and establish a direct link. This ensures that even when only the probability of the links between motes to share a key is 0.5, a fully secure communication network can be guaranteed 99.999% as long as multi-link paths of shared keys exist among neighbours [7].

III. Problem Definition and challenges

Providing security in IPv6/RPL connected 6LoWPANs is challenging because the devices are connected to the untrusted Internet and are resources constrained and the communication links are lossy [8]. The interest of this paper lies in Protocol Translation and End to End Security challenge [9]. The keys pre distribution algorithm suggested by [7] for Distributed Sensor Networks (DSN) was implemented for wireless sensors differs from a network of 6LoWPAN devices using RPL. This presents challenges such as in a DSN network if a mote does not share a key with one of its neighbours, it uses multi-link path to communicate with it, in contrast with IoT network where nodes are using RPL and each mote can communicate only with the mote that it form a leaf with. The limitations and constraints of the IoT devices also present another challenge in term of memory and processing power which mean a limitation in the size of keys, IDs and Rings.

IV. Proposed Approach

We propose to implement the Keys Pre Distribution for Distributed Sensor Networks DSN discussed in [7] on IoT devices network using RPL routing protocol. The key pre-distribution algorithm for DSN to the best of our knowledge was never tested on IoT devices using RPL routing protocol. We developed a simulation experiment to test our algorithm implementation.

V. Research & Experiment Methodology

The simulation was developed on the Contiki Operating System [11]. It uses many applications and tools designed specifically for low power lossy Networks and IPv6 devices such as Cooja [13] and Tunslip6 [11] The simulation experiment is looking at the performance of the key pre distribution algorithm proposed in [7] in the context of RPL.

The simulation experiment is looking specifically to explore the percentage of leaves in the RPL routing table that share a key. The sizes of bothe values are obtained using the same formulaes used in [7]. the key Ring and the Pool ranges from 8 keys in a key Ring when the Pool has 100 keys to 41 keys and in a key Ring when the Pool has 2500 keys. Those values are obtained using the same formulaes used in [7].

keys in the pool were generated and distributed thatto key Rings randomly using different Random techniques. Keys in the pool were generated using Blum Blum shub random number generator [14]. IDs were generated using Random library from C libary. Keys and IDs were distributed to differents Rings using knuth shuffle random algorithm [15].

VI. preliminary findings

The results of the simulation experiments shows that out of each pool used, a big proportion of the leaves

in the routing table shared a key as shown in figure 1 below[1]. For example, in figure 1 below, when the Pool contained a 1000 keys and the network was of 1000 motes, the percentage of motes in the DODAG that has a shared key was 54.01%. From the results obtained, it is clear that the internet of things devices when simulated achieve an average probability close to the 0.5% claimed. However this probability is not enough to achieve full connectivity of the network when using the RPL routing protocol since only a propotion of the leaves in the RPL table has a shared key and can communicate securly. However this leaves the remainder of the routing table leaves with unsecured links.

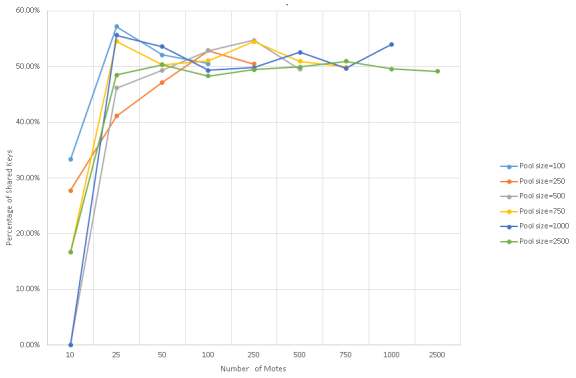

Fig. 1. Number of motes Vs Percentage of shared keys for various pools size

VII. Conclusion and Future Work

This paper investigated the performance of the key pre-distributed algorithm for distributed sensor networks on the IoT devices. The results obtained shows that the keys pre distribution algorithm when implemented on the IoT network using RPL does not achieve full secure connectivity in contrast with the DSN network in [7] since not all the RPL leaves are secured and thus not all motes in the RPL routing table are able to communicate.

The next step in this research will be to explore alternatives for solutions regarding leaves in the RPL routing table that do not share a key. A promising solution is to look at the Reactive Discovery of Point to Point routes in Low Power and Lossy Networks. [16].

[1]Percentage of shared keys for 10 or 25 motes in the network is low as motes are unable to communicate with each other

References

[1] Giancarlo Fortino & Paolo Trunfio, Internet of Things Based on Smart Objects: Technology, Middleware and Applications, Springer Publishing, 2014

[2] Rsao, et al., A Security Threat Analysis for Routing Protocol for low power and lossy Networks (RPL), Internet Engineering Task Force (IETF),draft-ietf-roll-security-threats-10, September 2014 https://tools.ietf.org/html/draft-ietf-roll-security-threats-10

[3] IEEE 802.15.4 Low Rate Wireless Personal Area Networks (LR-WPANs), IEEE standard for local and metropolitan area networks, USA, September 2011

[4] Zach Shelby & Carsten Bormann 6LoWPAN:The wireless embedded Internet-Part 1:Why 6LoWPAN?" EE Times,May 2011

[5] Hui & Vasseur, The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, IETF, RFC 6553 March 2012 https://tools.ietf.org/html/rfc6553

[6] Winter, et al. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, IETF, RFC 6550, March 2012 https://tools.ietf.org/html/rfc6550

[7] Laurent Eschenauer & Virgil D. Gligor, A key Managemenent Scheme for Distributed Sensor Networks,Proceedings of the 9th ACM conference on Computer and Communication security USA, 2002

[8] Linus Wallgren, Shahid Raza &nd Thiemo Voigt, Routing Attacks and Countermeasures in the RPL-Based Internet of Things, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 794326, 11 pages, June 2013. http://dx.doi.org/10.1155/2013/794326

[9] Alfred J. Menezes, Paul C. Van Oorschot and scott A. Vanstone, Handbook of Applied Cryptography, fifth edition, CRC press, August 2001. http://cacr.uwaterloo.ca/hac/

[10] Gradia-Morchon, et.al, Security consideration in the IP based Internet of Things, IETF, Internet Draft, March 2012

[11] Contiki Operating system http://contiki-os.org.

[12] Frederik Ostrelind, A sensor Network Simulator for the Contiki OS, February 2006 http://soda.swedish-ict.se/2296/1/SICS-T--2006-05--SE.pdf.

[13] Frederik Ostrelind, A sensor Network Simulator for the Contiki OS, February 2006 http://soda.swedish-ict.se/2296/1/SICS-T--2006-05--SE.pdf.

[14] Lenore Blum, Manuel Blum, Michael Shub, Comparison of two Pseudo -Random number generators,plenum, 1982

[15] Donald E Knuth, The art of computer programming, Volume 2, Seminumerical algorithms, Adison Welsey Reading, 1969

[16] Goyal, et al. Reactive Discovery of Point to Point Routes in Low Power and Lossy Networks, Internet Engineering Task Force, draft-etf-roll-p2p-rpl-07, January 2012 http://tools.ietf.org/html/draft-ietf-roll-p2p-rpl-07