A Lightweight Secure Object Tracking Protocol for Internet of Things

R. Veni
M. Tech. (Information Security) Student
Computer Science and Engineering
Pondicherry Engineering College
Puducherry (India)

K. A. Selvaradjou
Professor
Computer Science and Engineering
Pondicherry Engineering College
Puducherry (India)

ABSTRACT
The Internet of Things (IoT) raises to the ever-rising system of physical objects that feature an IPv6 address for internet connectivity and the message that takes place between these objects and other internet-enabled devices and systems. It is provided with unique identifiers and the ability to transmit data over a net. Among several issues, the tracking and tracing of the path travelled by objects is an important problem. Though, there exist many techniques to track the moving objects, many of them are unsafe. Hence, there is a need for secure tracking of the objects. A secure object tracking protocol should ensure the visibility and traceability of an object along the travel path to support the Internet of Things (IoT). The existing protocol is based on Radio Frequency Identification (RFID) system for global unique identification of IoT objects. The existing does not provide authentication of objects, leads to injection of fake objects. The energy consumption is high. The proposed protocol enhances secure object tracking using lightweight cryptographic primitives and modelled the protocol using Security Protocol Description Language (SPDL). The proposed protocol is intended to provide authentication, integrity, confidentiality and encryption. For ensuring secure object tracking, the proposed protocol uses the lightweight cryptographic primitives which uses the concept of Hash Message Authentication Code (HMAC) which is used to verify the authenticity of an object. The protocol is also based on Cooperative Message Authentication Code (CMAC) which is used to reduce energy consumption with less overhead. Through network simulation, the performance of the protocol is evaluated and found to be more secure and require less computation when compared with existing protocols.

Keywords
Internet of Things(IoT), Hash Message Authentication Code (HMAC), Cooperative Message Authentication Code (CMAC), Security Protocol Description Language (SPDL), Lightweight Secure Object Tracking Protocol (LSOTP), Secure Object Tracking Protocol (SOTP), Radio Frequency Identification (RFID).

1. INTRODUCTION
The Internet of Things (IoT) is a paradigm where all the "things" (objects, people and so on) around us can globally and actively identify, connect, sense and report itself to the system. This requires seamless unique identification of each things in IoT [1]. The IoT system needs to verify the travel path and ensure on-site tracking of an object's movement to ensure connectivity and visibility [2]. It is important also to collect information on the status of the object along the path to improve forecasting accuracy, which helps to formulate strategies, increase visibility and reduce object transit time for users. But, to reach these results, the IoT system should share and exchange information between objects and partners from several administrative domains along the path via wireless media [3]. A secure object tracking protocol should ensure that an adversary should not be able to compromise the privacy of the users or the objects while tracing and tracking things globally. In this paper, a lightweight secure tracking protocol is proposed to ensure the visibility and the traceability of an object along the path. The proposed protocol also ensures the correctness of the travel-path while protecting the privacy of the users [4]. The proposed protocol which enhances the security algorithm and minimize the energy consumption with less overhead [5]. The main objective are:

- To verify authenticity of an object
- A secure tracking protocol for IoT to improve objects visibility and traceability for users along the travel path.
- Security assurance of the IoT system by ensuring nonrepudiation, privacy protection for the system and users.
- To reduce energy consumption with less overhead

The rest of the paper is organized as follows Section II gives an overview of the related work and its limitations. Section III deliberates about design of proposed lightweight secure object tracking protocol and explained about the algorithm used in lightweight. Section IV presents the specific security evaluation metrics. Section V presents the preliminary results of the protocol through simulation and Section VI summarizes the conclusion of the work.

2. RELATED WORK
In this section, the existing similar protocols are compared based on cryptographic requirements. In Elliptic curve public key encryption, it does not satisfy non-repudiation and even though they have increased storage, only limited bytes are permitted [6]. In Hash function, it does not satisfy non-repudiation and only limited bytes are permitted [7]. In Public key encryption to generate signature it does not satisfy non-repudiation and need for special storage [8]. In Key based hash, it does not provide privacy of the system [9]. In a logistic system, the objects are typically marked with unique identifier (such as IP address) belonging to a specific user, the problem is to effectively: Track the object which would travel to a set of partners with an objective and record the path travelled by the object at run time. This involves the use of cloud environment and underlying IP network [10]. As the tracking happens on the IP network which is vulnerable for attacks, secure object tracking protocol (SOTP) need to be devised to counter the possible attacks such as:

- injection of fake objects,
- privacy of the system,
- non-repudiation etc.

To solve the above problems the system, need a protocol which should be lightweight because the sensor having some constraint such as less storage, less computation capacity, less battery life, etc. Based on the observation of related works, the existing algorithm has some of limitations as follows:

- It does not avoid impersonation
- The updating of every server should be done at all time of requesting and tracking the object
- Energy consumption is high.

3. PROPOSED SYSTEM

In this section, the proposed protocol lightweight secure object tracking protocol (LSOTP) which improves security level is based on Hash Message Authentication Code (HMAC) which mainly focuses to verify the authenticity of an object. Co-operative Message Authentication Code (CMAC) which is used for all server updates and to reduce the energy consumption with less overhead.

3.1 System Design

In this proposed system, the requester who makes a request of an object to track. Security Protocol description language (SPDL) provide the platform to create protocol for security purpose. Hash Message authentication code(HMAC) enables the cryptography between server and requester if the requester is authenticated it enables in the network otherwise it neglects. Co-operative message authentication code (CMAC) it performs to inform the newly added requester for the object. This enables one time verification. The overview of the proposed system is depicted as the architecture diagram in Figure.1.

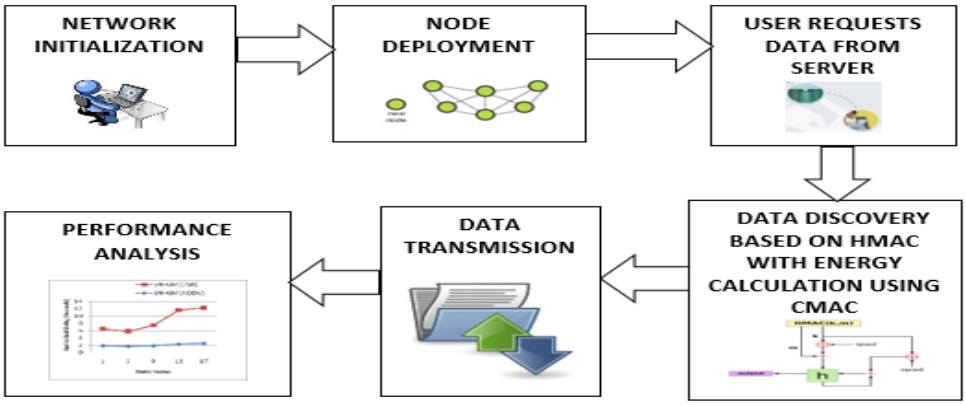

Fig.1 Architecture for Proposed System

3.2 Hash Message Authentication Code

Hash message authentication code (HMAC) is modified such way that satisfies the security properties. Hash functions are used to produce a fixed length digest of the input message. It is known as message digest or message authentication code. There have been several proposals to incorporate a secret key into an existing hash algorithm. The Pseudo code for the proposed HMAC algorithm is as follows:

1. *Set up the parameters*
2. *Input: the message M to HMAC (With necessary padding)*
3. *If K = B than Set K0: = K else if Go to step 9*
4. *End if*
5. *If K < B than K is padded with zeros in the left that form B byte string K0 else if Go to step 9.*
6. *End if*
7. *If K> B than hash the key K through H to get L byte string than add B-L zeros to get a B byte string. (i.e. K0=H (K) || 0000) else if Go to step 9.*
8. *End if*
9. *XOR K0 and ipad to generate a B byte string: K0 ipad*
10. *Append the input message to the output string. (K0 ipad) || M*
11. *Apply H to the stream generate in step 10. H ((K0 ipad) || M*
12. *XOR K0 and opad: K0 opad*
13. *Append the result of step 11 to result of step 12:*
14. *(K0 opad)|| H ((K0 ipad) || M)*
15. *Apply H to the stream generated in step 13 to get the final output:*
16. *H((K0 opad)|| H ((K0 ipad) || M))*

Where, B is Block Size (In Bytes) of Input Message, K is Secret Key (Shared by only sender and receiver), H is embedded hash function, ipad is Inner Pad: the byte 0x36 (In hexadecimal) repeated B times, K0 is Key K after necessary pre-processing (i.e. padded with zeros on the left) to form a B byte key, opad is Outerpad: 0x5C (In hexadecimal) repeated B times.

3.3 Working of HMAC algorithm

The size of the secret key K used in HMAC shall be equal to or greater than L/2. Here L is the size of Hash function output. If key size greater than the input block size (B bytes), first apply the key to hash function (H) than the resultant L byte string is used as a key. The Key should be chosen at random using key generation algorithms and change periodically. XORing of ipad and opad with key K result in the flipping of half of its key bits. But the flipped value will be different for ipad and opad respectively. Thus, two keys are pseudo randomly generated by key K. The graphical representation of the HMAC algorithm as shown in figure.2.

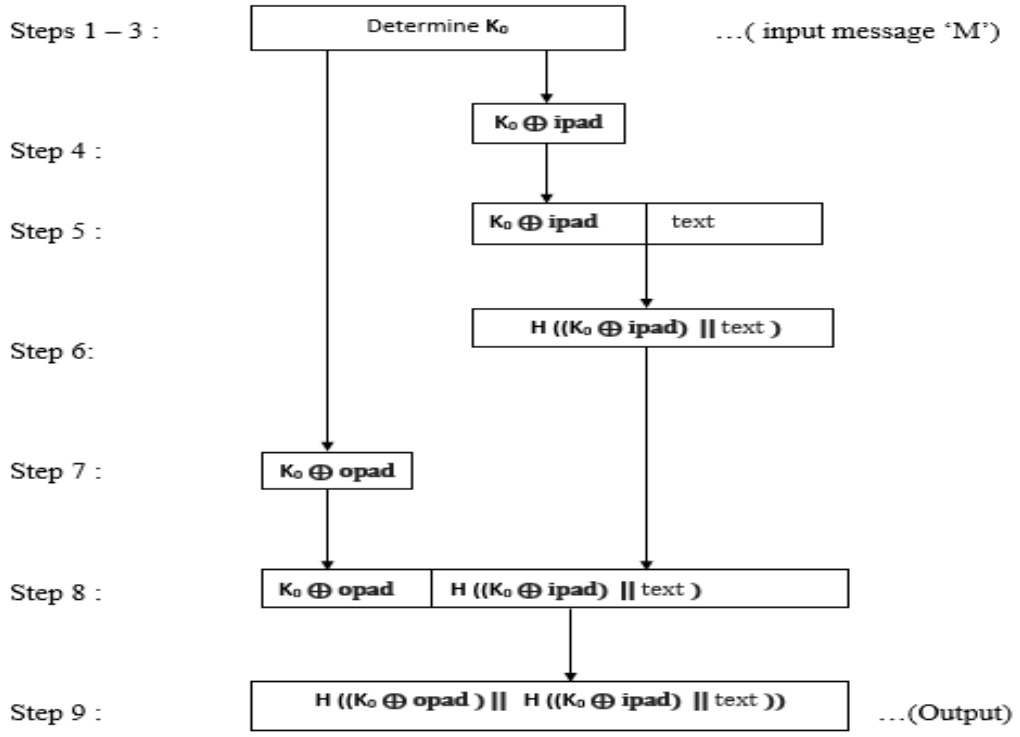

Fig.2 Graphical representation of HMAC algorithm

3.4 Cooperative Message Authentication code protocol

Cooperative message authentication code (CMAC) is verifying the group signature attached to each broadcast message is the dominating component that consumes computation capacity the average number of verified messages per object per second as the metric for the computation overhead. The CMAC introduces some extra communication overhead for dealing with the warning messages generated by the verifiers when an invalid broadcast message is detected. The average number of bits received by each object per second (i.e., the number of bits per object per second), which counts both the regular broadcast messages and warning messages. The percentage of the extra value of bits per object per second in the CMAC case relative to the bits per object per second in the non- cooperative case as the extra communication overhead of CMAC. CMAC method achieves significantly lower computation overhead. In fact, with the non-cooperative authentication protocol, each object verifies the broadcast messages from all its neighbours; while with CMAC, depending on whether the object is selected as a verifier, it verifies only a subset of the messages.

4. EVALUATION METRICS

In this section, the following specific security metrics are studied and compared the performance of existing and proposed protocols. The comparison of the proposed protocol with existing protocol based on security performance metrics are analysed by NS2 simulator.

4.1 Authorized Packets

It measures the number of authorized packets transmitted from source to destination and checks the packets which are received by the destination in authorized manner.

$$\textit{Authorized Packets} = \sum_i \frac{SRP_i}{(tsp_i - tst_i)} \quad (1)$$

Where, SPR_i – Number of successfully received packets, tst_i – Start Time, tsp_i – Stop Time, Unit- Packets

4.2 Unauthorized Packets

The number of unauthorized packets transmitted from malicious node. The packets which are not received by the destination in authorized manner.

$$\textit{Unauthorized Packets} = \sum_i \frac{\boldsymbol{RP}_i}{(\boldsymbol{tsp_i - tst_i})} \quad (2)$$

Where, RP_i—Number of rejected packets, tst_i – Start Time, tsp_i – Stop Time Unit- Packets.

4.3 Authentication Ratio

The ratio of the authorized packets vs unauthorized packets is called authentication ratio.

$$\textit{Authentication Ratio} = \sum_{i,j} \left(\frac{NA_j}{NU_i}\right) * 100 \quad (3)$$

Where, NA_j – Number of Authorized Packets, NU_i – Number of Unauthorized Packets, Unit - %.

4.4 Energy Consumption

The method achieves significantly less computation overhead. It is desirable to have a control packet and control information consumes energy. Energy consumption is the use of a system by making use of supply.

$$Energy\ Consumption = \sum_i \frac{CP_i}{(DP_i + CP_i)} \qquad (4)$$

Where, CP_i –Number of Control Packet, DP_i– Number of Data Packet, Unit – Joules.

5. SIMULATION RESULT

The proposed protocol has been implemented using NS-2.35 simulator. The simulation network consists of many sensor nodes distributed in a grid pattern of 1000×1000 m2. Each node is equipped with a radio transceiver capable of transmitting a signal over 250 m on a 2 Mb/s wireless channel. All applications are run on User Datagram Protocol (UDP). The simulated traffic is of Constant Bit Rate (CBR). The sink is assumed to be 250m away from the area.

Initial node energy is set as 2.7 Joules for the first set of simulations and 4.0 Joules for the second set of simulations.

The Channel Adaptive MAC protocol with Traffic Aware Dynamic Power Management scheme adopts the periodic sleep/listen operations, schedule selection and coordination, schedule synchronization, adaptive/listening and access control mechanisms of the protocol. The simulation parameters are shown in Table.1. The algorithm is examined and analyzed in the NS2.

Table.1. Simulation Parameters

Parameter	Value
Channel	Wireless Channel
Propagation	Propagation/TwoRayGround
Network Interface	Phy/WirelessPhy
MAC	Mac/802_11
Radio Range	Phy/WirelessPhy set RXThresh_ 2.13643e-07 Phy/WirelessPhy set CSThresh_ 2.13643e-07
Antenna	Omni-directional Antenna
Unique ID	IPv6
Routing Protocol	AODV
Node mobility	0 to 10m/s
Maximum Packet size	1000 bytes
Simulation Area	1200mX1200m
Traffic type	CBR
CBR packet size	512 bytes
Frequency	2.4GHz
Number of packets	30000
Pause time	1s
Simulation time	3000s
Number of Nodes	100

The proposed protocol is lightweight because it is having very less computation overhead and it is suitable for sensors, which are having very less resources such as less storage, less computation capacity, less battery life, etc. The protocol is secure because it uses concept of HMAC and CMAC. Finally evaluated the performance of the protocol for the following metrics: authorized packets, unauthorized packets, authentication ratio and communication overhead. Compare the performance of SOTP protocol with proposed protocol LSOTP with the following metrics. Ensuring that the proposed LSOTP protocol will achieve higher efficiency and provide reliable authorized packet when compared with the SOTP.

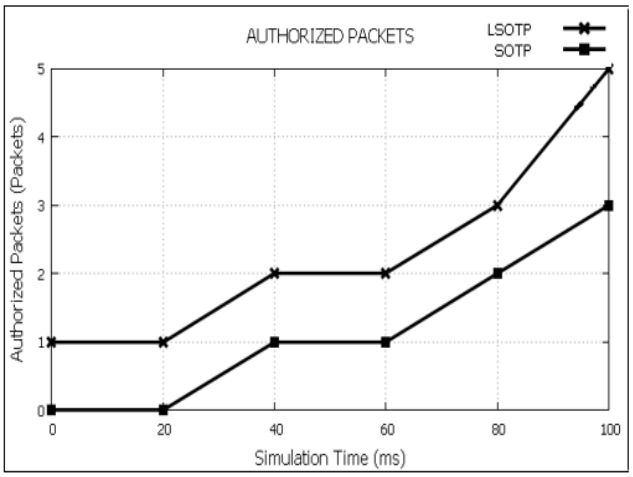

Fig.3 Simulation Result of Authorized Packets

The Figure.3 shows the authentication packets performance of the LSOTP compared with that of SOTP. The process of proving or showing something to be true, genuine, or valid.

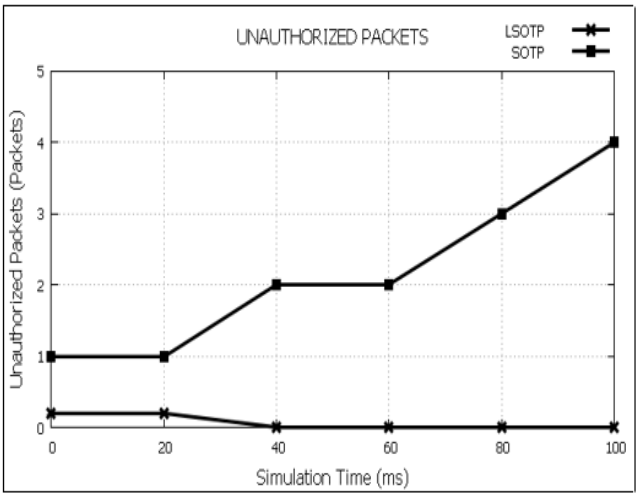

Fig.4 Simulation Result of Unauthorized Packets

The Figure.4 shows the unauthorized packets performance of a malicious node is defined as node seeking to deny service to other nodes in the network. The malicious packets are restricted here in lightweight secure object tracking protocol by using hash message algorithm. The unauthorized packets are minimized when compared with existing protocol.

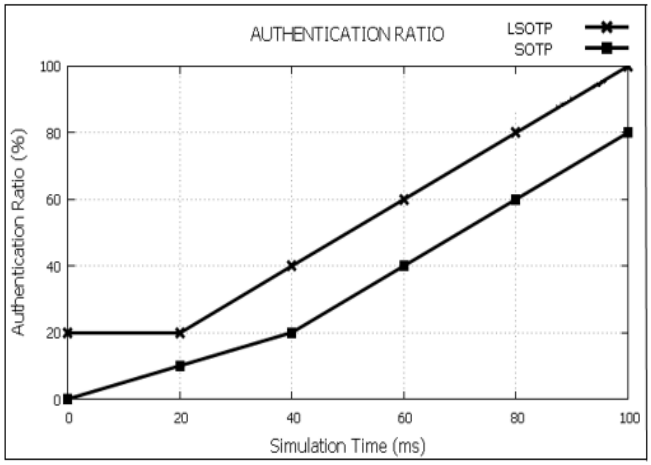

Fig. 5 Simulation Result of Authentication Ratio

The Figure.5 shows the authentication ratio performance of the LSOTP compared with that of SOTP.

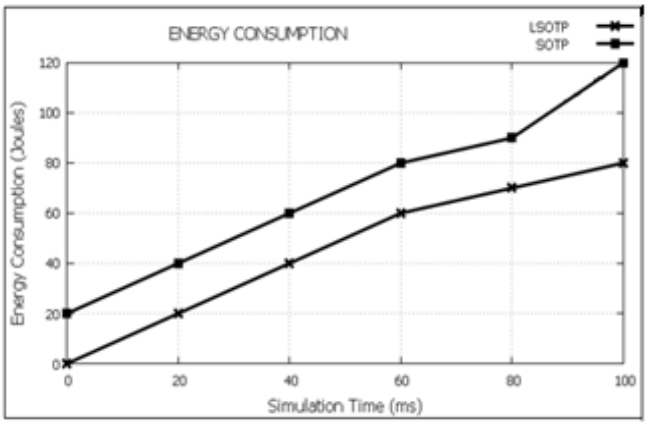

Fig.6 Simulation Result of Energy consumption

Accordingly, the simulation results shown in Figure.6 shows that the LSOTP gives better performance than SOTP irrespective of the security level. It is observed that LSOTP shows the improvement in energy consumption performance when compared with SOTP. By using LSOTP protocol the energy consumption is minimized with less overhead.

6. PERFORMANCE COMPARISON

The comparison of proposed protocol with existing similar protocol are compared based on security requirements and performance. Table.5.6 shows the results of the comparison. In addition, it shows that non-repudiation, privacy of the system was not secure and not satisfied by existing protocol.

The proposed protocol not only can realize the privacy protection but also can protect the confidentiality, authenticity and integrity of the object. The proposed lightweight secure object tracking protocol improved the security and reduced the energy consumption with less overhead.

7. CONCLUSION

The traceability and visibility of the object throughout its travel is considered an important problem in IoT. While doing so, the protocol should ensure security such as privacy, injection of fake objects and non-repudiation. A lightweight secure object tracking algorithm has been proposed in this project. The proposed algorithm uses HMAC and CMAC authentication protocols. Through extensive simulations it is shown that the LSOTP outperforms the existing SOTP. Due the high privacy and energy efficiency, the life time and the overall performance is improved. The scope for future work, Internet of Things (IoT) has opened many opportunities in both research and business. It has also presented many interesting technical challenges. The approach is to formulate practical problems in ways that make them amenable to theoretical treatment. Such a rigorous and mathematical approach leads to many insights that help one better understand. The research approach provides a promising and crucial voice to this new frontier of large-scale.

Table.2. Comparison based on security requirements

Protocol	Security Requirements				
	CF	**IFO**	**P**	**NR**	**EC**
SOTP (Existing)	Hash function	**X** **(**does not satisfy the titled description)	Δ (partially satisfied)	Δ (partially satisfied)	**X** **(**does not satisfy the titled description)
LSOTP (Proposed)	Hash function, Security Key, Security Packet and Cryptography	√ (protocol satisfies the titled description)	√ (protocol satisfies the titled description)	√ (protocol satisfies the titled description)	√ (protocol satisfies the titled description)

CF: Cryptographic Functions, **IFO**: Injection of Fake Objects, **P**: Privacy of the system, **NR**: Non-Repudiation, **EC**: Energy Consumption.

8. REFERENCES

[1] Stankovic, J. A. "Research directions for the internet of things" *IEEE Internet of Things Journal*, vol. 1, no.1, pp.3-9, February,2014.

[2] Kumar, Hemant, and Archana Singh. "Internet of Things: A Comprehensive Analysis and Security Implementation through Elliptic Curve Cryptography", In *International Journal of Current Engineering and Technology (IJCET)*, March ,2016.

[3] Ray, B., Howdhury, M., Abawajy, J., and Jesmin, M. "Secure object tracking protocol for Networked RFID Systems" *In the Proceedings of 16th IEEE/ACIS International Conference of the IEEE on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 1-7, June,2015.

[4] Sankaran, S "Lightweight security framework for IoTs using identity based cryptography*" In the Proceedings of IEEE International Conference* on *Advances in Computing, Communications and Informatics (ICACCI)*, pp. 880-886, September,2016.

[5] Jiang, S., Zhu, X., and Wang, L."An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs" *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193-2204, August,2016.

[6] Elkhiyaoui, K., Blass, E. O., and Molva, R. "CHECKER: On-site checking in RFID-based supply chains" *In the Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, pp. 173-184, April,2012.

[7] Blass, E. O., Elkhiyaoui, K., Molva, R., and Antipolis, E. S. "Tracker: Security and privacy for RFID-based supply chains" *In the Proceedings of 18th Annual Network and Distributed System Security Symposium*, pp. 6-9, February,2011.

[8] Burbridge, T., and Soppera, A. "Supply chain control using a RFID proxy re-signature scheme", *In the Proceedings of IEEE International Conference on RFID*, pp. 29-36, April,2010.

[9] Ouafi, K., and Vaudenay, S. "Pathchecker: An RFID application for tracing products in supply-chains", *In the Proceedings of RFID Sec*, July,2009.

[10] Ray, B. R., Chowdhury, M. U., and Abawajy, J. H. "Secure Object Tracking Protocol for the Internet of Things", *IEEE Internet of Things Journal*, vol. 3 no. 4, pp. 544-553, August,2016.