JES Journal of Engineering Sciences

Vol 11, Issue 6,June/2020
ISSN NO:0377-9254

A Survey on Reliable Handoff Mechanism for Energy Efficient Internet of Things Wireless Sensor Networks

Dr.Ruksar Fatima[1] and Nishatbanu Nayakwadi[2]

[1]Professor & Vice Principal, Dept. of Computer Science & Engineering, K,B.N College of Engineering, Kalaburgi, Karnataka,India,ruksarf@gmail.com
[2]Research Scholar Dept. of Computer Science & Engineering K.B.N College of Engineering, Kalaburgi, Karnataka,India,nishatbanu7777@gmail.com

***ABSRACT*--- The communication is very sensitive and crucial in Smart Home-IoTs (SH-IoT) such as electronic devices and sensors. Additionally, the key requirement of SH-IoT consist the channel security, mobility management, consistent data rates and handover support. The PMIPv6 (proxy mobile IPv6) is included as the one of core solutions to manage the extreme mobility. However, in SH-IoT scenarios the default PMIPv6 cannot confirm the performance enhancement such as the RO (Route Optimization). The present security protocols for smart home of IoT services cannot confirm the RO for PMIPv6, where the MNs (mobile nodes) interconnect with *home* of IoT devices that is not belonging to domain. The secure protocol has proposed in which the user trust among the smart home and PMIPv6 domain to confirm the security as well as the performance over the path among the IoT devices and MNs. The proposed protocol contains the step for handover management and secure RO, such as key exchange, privacy, perfect forward security; mutual authentication and privacy are supported. The propose protocols of correctness is formally examined utilizing automated validation and BAN-logic of AVISPA. Later, the simulation of network is conducted to estimate the proposed protocol of performance of efficiency. An outcome represents the proposed approach that is capable of providing the secure transmission by solving the RO issue in PMIPv6 along with the deduction in handover latency, packet loss, enhancement and end to end in transmission rate and throughput during the handover phase.**

Keywords: **SH-IoT, PMIPv6, Route Optimization (RO), Local mobility anchor, Mobile access gateway.[1]**

1. INTRODUCTION:

Nowadays, the desire for a smart society that utilizes technologies such as large-scale sensor networks [1], the Internet of Things (IoT) [2], and smart skins [3], [4] is continuously growing. One of the most pressing issues is the lack of a sustainable power supply that could enable the autonomous operation of these sensors and devices (motes). Conventional autonomous devices heavily rely on primary batteries, which can power the devices for only a certain amount of time. Once the sensor devices use up the stored energy in their batteries, the batteries need a replacement at a cost that increases significantly as the number of sensor devices in the system increases. To avoid this maintenance cost issue and achieve completely self-sustainable low-cost ubiquitous systems for the IoT and smart cities, research communities have devoted a considerable interest in ambient energy saving technologies.

The Internet of Things (IoT) paradigm envisions a wide infrastructure network of "things" that forms a pervasive computing environment [5]. It is defined as a global network with an infrastructure that has self-configuring capabilities [6]. IoT is an intelligent network that connects billions of things via the Internet by using a variety of communications technologies such as conventional Long Term Evolution (LTE), Wi-Fi, ZigBee, wireless sensor networks (WSNs), Ethernet, as well as specially developed Internet Protocol Version 6 (IPv6) over low-power wireless personal area networks (6LoWPAN), the low-power wide area network from the LoRa Alliance (LoRaWAN), LTE machine type communications (LTE- MTC), narrowband IoT (NB-IoT), and many other communications technologies. Therefore, the IoT is rapidly transforming into a highly heterogeneous ecosystem that provides interoperability among different types of devices and communications technologies. Many

interconnected objects will be able to sense physical phenomena and exchange data, information and knowledge through the network, to leverage the user experience of the surrounding environment. Energy efficiency is a key aspect for these IoT battery-powered devices, which feature sensing, communication and processing capabilities.

The IoT achieves the goal of intelligent identification, location, tracking, monitoring, and managing of things [7]. It also creates additional value for a better life by sharing the information collected among different things, and it integrates and consolidates services at the edge using different Io gateways. IoT implementation requires new solutions to integrate different physical objects (things) into a global IoT ecosystem so that all of them can be identified and recognized automatically.

Therefore, IoT is simply M2M (machine-to-machine) communications, sensor node is reportedly the most appropriate for this new technology. One of the most important features of IOT devices is that they can communicate with each other in very low power and possess very less overhead. Hence, data handover in these low-power devices can be efficient and data loss probability can be minimized. Therefore, to communicate with sensor node and handle such huge data, the use of IoT devices can prove an effective solution. The default PMIPv6 based on the SH-IoT network that allows a MN to interact with CNs (Corresponding nodes), which are the devices of IoT in home, regardless of movement and location through MAG (Mobile access gateway), LMA (Local mobility anchor) and intermediate entities [8] as shown in Fig.1. In PMIPv6 a SH is composed of devices of SH-IoT and HGW which is based on SH-IoT, and every devices relies on the HGW to interact with external entities consisting MNs. It can be noticed in Fig1 that each message which is send to the CN, that follows a non-optimal path between the LMA and MAG and the HGW which is leading to the performance of excessive overheads. Additionally, whereas the handover decision is made, replication of all procedure via the path of MAG-LMA-HGW maximizes the handover latency, that affects the all performance of network. The above issues are maintained which is raise the need of RO. Here, the worth RO is noted, if not secured adequately and vulnerable to different security threats [9]. To consider the security aspects that there are 3 possible trusts recognized in PMIPv6 based on networks of SH-IoT, and trust among the MAG and MN, LMA and MAG, CN and HGW. Unfortunately, those trusts are not enough to gain the secure RO during they cannot permit a HGW and MAG to negotiate and authenticate each other in session key. In other hands, it is not possible to give secure RO, which is based on the present possible trusts. Hence, the excessive dependency of elimination over the LMA for every transmission, even and after the authentication, this problem statement is as well as the motivation behind the need of solution for secure RO in applications of smart home.

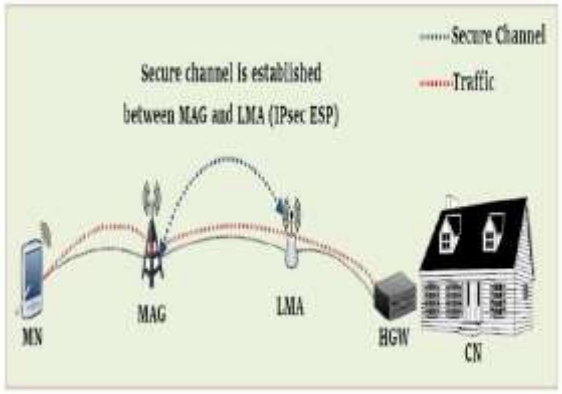

Fig1. The default PMIPv6 based SH-IoT networks

2. LITERATURE SURVEY:

In [10] with the advancements in wireless technology and digital electronics, some tiny devices have started to be used in numerous areas in daily life. These devices are capable of sensing, computation and communicating. They are generally composed of low power radios, several smart sensors and embedded CPUs (Central Processing Units). These devices are used to form wireless sensor network (WSN) which is necessary to provide sensing services and to monitor environmental conditions. In parallel to WSNs, the idea of internet of things (IoT) is developed where IoT can be defined as an interconnection between identifiable devices within the internet connection in sensing and monitoring processes. This paper presents detailed overview of WSNs. It also assesses the technology and characteristics of WSNs. Moreover, it provides a review of WSN applications and IoT applications.

Internet of Things (IoT) is not only a promising research topic but also a blooming industrial trend. Although the basic idea is to bring things or objects into the Internet, there are various approaches, because an IoT system is highly application

oriented. This paper [11] presents a wireless sensor network (WSN)-based IoT platform for wide area and heterogeneous sensing applications. The platform, consisting of one or multiple WSNs, gateways, a Web server, and a database, provides a reliable connection between sensors at fields and the database on the Internet. The WSN is built based on the IEEE 802.15.4e time slotted channel hopping protocol, because it has the benefits such as multi-hop transmission, collision-free transmission, and high energy efficiency. In addition to the design of a customized hardware for range extension, a new synchronization scheme and a burst transmission feature are also presented to boost the network capacity and reduce the energy waste.

Connecting physical objects-devices, vehicles, buildings and other items to the internet with the help of embedded electronics, software, sensors and network operations in order to collect and analyze data and for data exchange among these devices is called as IOT. In general connecting all the devices to the internet and trying to operate them remotely. In this paper [12] a review on the data collection in IOT and decision making principles are presented.

[13] Wireless Sensor Networks (WSN) and the Internet of Things (IoT) are composed of devices capable of sensing/actuation, communication and processing, that could be used to improve our daily life, however standardization has been considered one of the main challenges to their deployment. We here discuss standardization issues and possible uses of Software-Defined Networking (SDN) in the context of the Internet of Things. They provide an overview of RPL and TinySDN protocols, and then examine their routing features, interoperability possibilities and support to legacy networks.

In the near future, the IPv6 protocol [14] is expected to provide internet connectivity to any object embedding a communication device, by creating the so-called Internet of Things (IoT). In this scenario, IPv6 Wireless Sensor Networks (WSNs) have a key role since they can be used to collect several environment information, hence becoming the eyes, ears and nose of the IoT. Since wireless sensors are limited in power, it is essential to design energy efficient WSNs protocols. To this purpose, in this paper, we propose a Resource Oriented and Energy Efficient (ROEE) routing protocol based on the Routing Protocol for Low power and Lossy networks (RPL). ROEE RPL is intended as the very first building block to achieve the so called IoT[15] Maintaining critical data access latency requirements is an important challenge of Industry 4.0. The traditional, centralized industrial networks, which transfer the data to a central network controller prior to delivery, might be incapable of meeting such strict requirements. In this paper, we exploit distributed data management to overcome this issue. Given a set of data, the set of consumer nodes and the maximum access latency that consumers can tolerate, we consider a method for identifying and selecting a limited set of proxies in the network where data needed by the consumer nodes can be cached. The method targets at balancing two requirements, data access latency within the given constraints and low numbers of selected proxies. We implement the method and evaluate its performance using a network of WSN430 IEEE 802.15.4-enabled open nodes. Additionally, we validate a simulation model and use it for performance evaluation in larger scales and more general topologies.

IN [16] In order to promote the development of the IoT, the Internet Engineering Task Force (IETF) has been developing a standard named Internet Protocol Version 6 (IPv6) over Low Power Wireless Personal Area Networks (6LoWPAN) to enable IP-based devices to connect to the Internet. Besides, to support mobility management, a network-based localized mobility management (NETLMM) protocol named Proxy Mobile IPv6 (PMIPv6) is proposed. Although the 6LoWPAN standard has specified the important issues, some security and mobility issues have not been addressed. In this paper, a secure PMIPv6-based mobility scheme is designed. The proposed scheme enables a 6LoWPAN device to efficiently and securely roam in the 6LoWPAN networks.

In [17], the communication in the Smart Home Internet of Things (SH-IoT) comprising various electronic devices and sensors is very sensitive and crucial. In addition, the key requirements of the SH-IoT include channel security, handover support, mobility management, and consistent data rates. Proxy mobile IPv6 (PMIPv6) is considered as one of the core solutions to handle extreme mobility; however, the default PMIPv6 cannot ensure performance enhancement in SH-IoT scenarios, i.e., Route Optimization (RO). The existing security protocols for PMIPv6 cannot support secure RO for smart home IoT services, where mobile nodes (MNs) communicate with home IoT devices not belonging to their domain. Motivated by this, a secure protocol is proposed, which uses trust between PMIPv6

domain and smart home to ensure security as well as performance over the path between MNs and home IoT devices. The proposed protocol includes steps for secure RO and handover management, where mutual authentication, key exchange, perfect forward secrecy, and privacy are supported.

3. PROBLEM STATEMENT:

Extensive research survey is carried out shows that the minimization of energy consumption in IoT devices will be a challenging task for future wireless sensor technology. The increase adoption of 4G cellular network topology for various service provisioning and the 5G cellular network topology is expected to be by 2022 will further increase more challenges in IoT devices and wireless sensor networks. Data transmission and handover between IoT devices in real time is difficult process due to high-energy consumption, long transfer delays, large data loss, and high overhead and significant processing costs. Many approaches are presented in recent years to address these issues; however, these are limited to generation low latency and high speed. However, minimization of energy consumption, elimination of overhead and secured data handover etc. becomes unsolved issues. In many existing approaches, various sensing techniques are adopted based on clustering, use of low power sensing cameras and routing optimization techniques etc. However, only few techniques can be adopted in real time for future use due to its high computational complexity, missing data, delay, high-energy consumption and latency. Therefore, overall energy minimization in IOT devices cannot be achieved.
The future wireless sensor network is expected to be highly dense due to use of IoT devices and 5G cellular network topologies. Therefore, energy minimization needs to be considered in IoT devices for wireless sensor networks while handover.

4. PROPOSED METHOD:

The objective of the research work proposed is to propose an efficient handover mechanism for IoT devices and resolve issues of existing algorithms.

- To review the existing handoff mechanisms in detail with their research contribution and limitations/research gap.
- To achieve an efficient handoff management for IoT and other advanced devices will be introduced while maintaining high QoS.
- First, we will eliminate noise to get large sensor data values and ensure no loss of data.
- To provides better quality of service, minimizing the cost to the network, when handoff occurs during execution owing to the user's movement, compared with other mobility management protocols.
- Our model will be evaluated under different environmental condition

.

5. STUDY AREA AND METHODOLOGY:

The study area of proposed research work is internet of things (IoT). IoT is a present hot topic in area of research. The potential benefits of IoT are almost limitless and IoT applications are changing the way we work and live by saving time and resources. It opened a new opportunities for growth, innovation and knowledge creation. IoT helps public and private sector organization to manage assets, optimize performance and develop new business model. As a vital instrument to connect devices and to act as a generic enabler of the hyper connected society IoT has a great potential to improve energy efficiency, to support aged society and to optimize all kinds of mobility and transport. In order to reach full potential of an IoT services flexibility and security are key requirements. For multiple service areas such as supply chain or aftermarket service, access control and secure dispatch of information play a major role. Thus we need secure service handover of smart devices from one security domain to another security domain. The research work related to hand over management of sensor data in IoT devices and existing data delivery techniques those comprehensively studied. The related research work has been critically analysed for deriving the new model for the present research work. The envisioned Handover management in IoT devices is shown in Fig.2

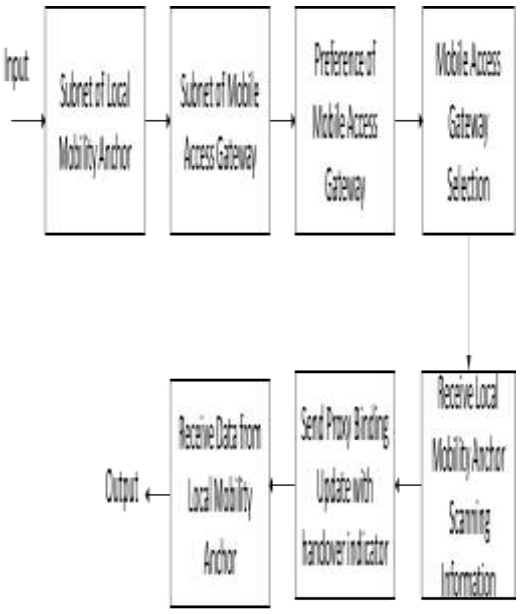

Fig2. Handoff mechanism in IoT devices

The terminologies used in Fig.2. can be explained as:

- Local Mobility Anchor (LMA):

Local Mobility Anchor (LMA) is the home agent for a mobile node (MN) in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for MN home network prefixes and manages the binding state of an MN. An LMA has the functional capabilities of a home agent as defined in the Mobile IPv6 base specification (RFC 3775) along with the capabilities required for supporting the PMIPv6 protocol.

- Mobile Access Gateway (MAG):

The Mobile Access Gateway is a network relay that provides a secure and effective method for individual applications to access corporate resources. When user access internal content from their mobile devices, the MAG ensures a secure transfer between the device and enterprise system. The MAG is able to authenticate and encrypt traffic from individual applications on compliant devices to the back-end system they are trying to reach.

- Proxy Binding Update (PBU):

The proposed scheme is based on the PMIPv6 bulk binding update mechanism which is designed to optimize the binding update and revocation operations for a group of mobility sessions by introducing group identifier. The group identifier can be assigned by MAG or LMA and will be exchanged via Proxy Binding Update (PBU) and Proxy Binding Acknowledgment (PBA) messages and generally used to extend the lifetimes of multiple mobility sessions and revoke all the sessions hosted on the failed service card

.

6. EXPECTED OUTCOME:

i. The proposed model will minimize latency thus improving the handover mechanism in IoT devices.
ii. The proposed handoff algorithm for IoT devices can provide reliable wireless sensor data delivery packet
iii. The proposed model can reduce the different noises and overhead present in the existing networks.

7. CONCLUSION:

In this article, first provide the Efficient-communication in the networks of SH-IoT that was considered in RO, and proposes the secure protocol, which utilized the domain of PMIPv6 divisibility to confirm the security as well as the performance over the path between the CN and MN. As proved here the analytical model implementing the O-PMIv6 provides the network operator a large number of developments to the several performance factors as such localized routing, delay of handover and LMA utilization. This is very vital in the real network deployment in that the mobile nodes are expected to the fast moving nodes, which have localized routing development with their remote of CN. Additionally the O-PMIv6 exhibits the similar advantages over the PMIPv6 in terms of the packet loss rate and handover delay. Our upcoming days the work is to study the utilization of O-PMIPv6 for the scenario where more than one LMA PMIPv6 domains are involved.

8. REFERENCES:

[1]. H. Nishimoto, Y. Kawahara, and T. Asami, "Prototype implementation of ambient RF energy harvesting wireless sensor networks," in Proc. IEEE SENSORS, Nov. 2010, pp. 1282–1287. [Online].

[2]. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online].

[3]. L. Gao et al., "Epidermal photonic devices for quantitative imaging of temperature and thermal transport characteristics of the

skin," Nature Commun., vol. 5, p. 4938, Sep. 2014. [Online].

[4]. B. S. Cook, T. Le, S. Palacios, A. Traille, and M. M. Tentzeris, "Only skin deep: Inkjet-printed zero-power sensors for largescale RFID-integrated smart skins," IEEE Microw. Mag., vol. 14, no. 3, pp. 103–114, Mar. 2013. [Online].

[5]. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[6]. R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)", IEEE Internet Initiative, Torino, Italy, 2015.

[7]. K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview", The Internet Society (ISOC), October 2015.

[8]. S. Gundavelli, V. Devarapalli, K. Chowdhury, and B. Patil, ``Proxy Mobile IPv6," IETF RFC, USA, Tech. Rep. 5213, Aug. 2008, p. 93. [Online]. Available: https://tools.ietf.org/html/rfc5213.

[9]. I.You, J.-H. Lee, and B. Kim, ``caTBUA: Context-aware ticket-based binding update authentication protocol for trust-enabled mobile networks," *Int. J. Commun. Syst.*, vol. 23, no. 11, pp. 1382_1404, 2010.

[10]. M. Kocakulak and I. Butun, "An overview of Wireless Sensor Networks towards internet of things," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-6.

[11]. Y. Kuo, C. Li, J. Jhang and S. Lin, "Design of a Wireless Sensor Network-Based IoT Platform for Wide Area and Heterogeneous Applications," in IEEE Sensors Journal, vol. 18, no. 12, pp. 5187-5197, 15 June15, 2018.

[12]. K. Begum and S. Dixit, "Industrial WSN using IoT: A survey," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 499-504.

[13]. B. Trevizan de Oliveira, R. C. A. Alves and C. Borges Margi, "Software-defined Wireless Sensor Networks and Internet of Things standardization synergism," *2015 IEEE Conference on Standards for Communications and Networking (CSCN)*, Tokyo, 2015, pp. 60-65.

[14]. Barbato, M. Barrano, A. Capone and N. Figiani, "Resource oriented and energy efficient routing protocol for IPv6 wireless sensor networks," *2013 IEEE Online Conference on Green Communications (OnlineGreenComm)*, Piscataway, NJ, 2013, pp. 163-168.

[15]. Theofanis P. Raptis,*Andrea Passarella, and Marco Conti, "Performance Analysis of Latency-Aware Data Management in Industrial IoT Networks", 2018 Aug; 18(8): 2611.

[16]. Y. Qiu and M. Ma, "A PMIPv6-Based Secured Mobility Scheme for 6LoWPAN," *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, 2016, pp. 1-6.

[17]. Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks. IEEE Access, 5, 11100–11117