International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 6, June 2015

Security Aspects At The Junction Of MANET And Internet Of Things

[1] Mamata Rath, [2] Umesh Prasad Rout,
[1]C. V. Raman Computer Academy, Bhubaneswar, Odisha [2]School of Information and Computer Science
[1] mamata.rath200@gmail.com [2] umesh.upr@gmail.com

***Abstract:*— In the current technology the Internet of Things (IoT) is developing as a promising trend towards interconnecting physical objects. Conceptually the IoT provides a platform to enable the objects to interact with each other or with end users by forming network of interconnected things. Recent advancement in Mobile Adhoc Networks (MANET) which enables dynamically formation of network and networking without pre-defined infrastructure shows great success incorporating many IoT based application domain in smart cities. Internet of things (IoT) and ubiquitous computing, such as MANET becomes increasingly popular in current technology. In this paper major security aspects are discussed due to handshaking of IoT with MANET and issues related to IoT based applications in MANET are analysed with special focus on need of smart protocols for smart environment.**

Keywords: **IoT; MANET; Smartcity; Ubiquitous Computing ; Routing Protocol**

I. INTRODUCTION

With rapid increase of internet users, more people have access to global information and communication technology, as a result of which the issues of using internet as a global platform and enabling the smart objects and machines to co-ordinate, communicate, compute and calculate gradually emerges [1].

Every day billions of people across the world use Internet for browsing and accessing the world wide web for many purpose like send and receive email, download high volume audio and video files, games, animation using social networking sites etc. In the same time another problem of use of internet as a common platform for communication and message transmission by smart objects and co-ordination among them also gradually increases. In this context, the term ‘‘Internet-of-Things’’ (IoT) is basically used to refer smart objects with advanced Internet Technology and all supporting technology used to realize such ideal vision and to put together properly application and service technology to open new business opportunity.

II. SECURED ROUTING IN MANET AND INTERNET OF THINGS

It is very much essential to design highly efficient and secured routing protocols for both MANET and IoT. Cryptographic techniques are used in many secured routing for security of mobile nodes by authentication at every hop during hop-to-hop transmission[1]. Authentication mechanism are carried out among the nodes and t every intermediate nodes to cryptographically ensure after checking the digital signatures which are attached to the encrypted routing information. Sometimes a trust metric is used as the parameter to check authenticity of the data packets. The final objective of having secured protocol is to store more valid information to the routing messages, efficiently calculating the routing table updates and other security based operations that are embedded into the routing protocols thereby securing it most. Excessive overhead sometimes makes inefficient decisions. So the final objective is to design energy and delay efficient routing protocols for IoT environment keeping all the possible security aspects into consideration.

III. RELATED WORK

As per paper [2], IoT technology views all the objects in the inter connected world as virtual objects.Such objects can be either devices, services and processes which are capable of offering methods to remain connected to the Internet. So IoT is a part of the future Internet which can be understood as a paradigm which integrates different technological solutions. So there is a need of standard transmission protocols which can support this particular aspect of IoT. Authors in [3] describe that MANET can be understood as a self-organised and self configured group of mobile nodes in a wireless network capable of doing communication with each other dynamically. Now a days this important ubiquitous computing along with IoT technology gradually becomes popular as this pair of network environment work efficiently on Smart Objects. According to [4], wireless networks such as WSN and MANETs have become the main technology for many IoT applications and similar domains in smart cities. Due o

their self configuration ability their role in IoT has become more efficient. These application areas ranges from academic interest to research and very soon these combined technology is going to be implemented in Environment Monitoring, traffic management and for public safety related systems.

IV. SECURITY ASPECT AT THE JUNCTION OF MANET & IoT-

1.Incorporation of secured MANET Routing Protocol in IoT –

It is a very challenging task to manage security at the IoT environment as here many heterogeneous devices are networked together. Current research shows that the networks due to IoT are prone to many attacks such as malware,botnets,DoS (Denial of Service) attack , Web based malware, android malware and spam.Therefore there is need of developing a standard secured frame work for communication in IoT [5].

2.Security aspect of IoT satisfying Confidentiality-

The basic requirement of Internet of Things which is also any kind of Adhoc Network is availability , authenticity and non-repudiation which are features of basic security regulations. Confidentiality refers to the feature that ensures that information should never be revealed to the wrong source. In MANETs, there is security provisions not to allow malicious nodes to get unauthorized access to important information regarding routing neither from any genuine node or while the transmission goes on this information does not reveals outside. Similarly another feature of security Integrity refers to conforming the data accepted by destination node should not be directed to wrong destination while in transit.

3.Secured Routing in MANETs and IoT

Designing secure and efficient routing protocols for MANETS is a primary challenge but, extremely useful in maintaining network route information and security.Cryptographic techniques are used to keep the routing information secured during the transmission. Security protocols are embedded in routing mechanism to authenticate and validate the packets during hop-to-hop transmission. All intermediate nodes are required to authenticate and check the digital signature attached with the packets before forwarding to the next hop node.

4.Design of secured communication scheme for IoT in MANET Environment

In Communication system used in battle fields, tanks, ground soldiers and real time aerial vehicles comprises a IoT network where MANET technology used for communication. A password based group key exchange system was developed by Byun in 2006 for such network. A more developed password based communication scheme is proposed in [6] for IoT environment that can be used in battle field and it supports dynamic group scheme. In this method the group nodes of the heterogeneous MANET understand the broadcast message and direct communication is possible in real time systems. Simulation of this scheme proves that it is dynamic and robust.

5. SDN (Software Defined Networking) Architecture for IoT-

In Software Defined Networking Architecture the main importance is given to the network statistics such as transmission rate, bandwidth consumption rate, delay rate[7]. Whereas in IoT due to multiple networking, state information about many devices are stored in a loosely coupled manner over the distributed network. To measure the performance of IoT network it is difficult to select a parameter just like band width consumption etc due to heterogeneous type and time-sensitive issue of different data types.

In recent technology SDN techniques are mostly used in wireless network. In [7] an innovative multi-network controlling system and its architecture is designed to choose a better performance metric in IoT network. The data collection component and device related information from the multi-networking environment of IoT and the information are stored in the database. Then the information is used by the layered component. The Analyst also controls the process by incorporating external software tools to the system. Conceptually the controller is centralized to improve the throughput as per increase of large volume of data.

V. CONCLUSION

Due to the Emergence of MANET equipped IoT technology, prompt communication and interaction among Smart Objects in a highly mobile and dynamic environment has been successfully achieved. Handshaking of MANETs with IoT play significant role in many challenging and advanced application domains like smart cities, traffic Management, controlling, monitoring and Logistics. In this context a complete study and analysis has been carried out regarding the security aspects of this handshaking technologies and challenging issues at their junction point. Such analysis

will definitely encourage the need of development of more secured, challenging and intelligent routing protocols at the intersection of MANETs and IoT.

REFERENCES

[1] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, "Internet of things: Vision, applications and research challenges ",Ad Hoc Networks ,Vol 10,Pages 1497–1516,2012.

[2]Daniel G. Reina , Sergio L. Toral, Federico Barrero, , Nik Bessis, , Eleana Asimakopoulou "The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments",Chapter, Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence, Vol 460,Pages 89-113, ISBN: 978-3-642-34951-5 (Print) 978-3-642-34952-2 (Online)-2013.

[3] Shuaishuai Tan, , Xiaoping Li , Qingkuan Dong , Trust based routing mechanism for securing OSLR-based MANET", Adhoc Networks Volume 30, Pages 84–98, July 2015.

[4] Paolo Bellavista, Giuseppe Cardone,Antonio Corradi, Luca Foschini," Convergence of MANET and WSN in IoT Urban Scenarios", IEEE Sensors Journal, Vol. 13, No. 10, Oct 2013.

[5] David Airehrour, Jairo A. Gutierrez, "An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT Routing", .http://www. researchgate. net/ publication /277078202, Last accessed on - August 2015.

[6] Zhang Hua,Gao Fei,Wen Qiaoyan" A Password-Based Secure Communication Scheme in Battlefields for Internet of Things", China Communications, Vol.8,Issue 1,Pages 72-78,2011.

[7] Zhijing Qin, Denker, G., Giannelli C., Bellavista P. Venkata subramanian, N., "A Software Defined Networking architecture for the Internet-of-Things," in Network Operations and Management Symposium (NOMS), Pages 1-9, 5-9 May 2014.

[8] Silva,R.; SaSilva,J.; Boavida,F."
A symbiotic resources sharing IoT platform in the smart cities context"Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on, Year: 2015.

[9] Yan Sun Jingwen Bai , Hao Zhang , Roujia Sun, Chris Phillips ," A Mobility-Based Routing Protocol for CR Enabled Mobile Ad Hoc Networks", International Journal of Wireless Networks and Broadband Technologies (IJWNBT),Vol 4, Issue 1, 2015.

[10] Caroline Chibelushi1, Alan Eardley, Abdullahi Arabo," Identity Management in the Internet of Things: the Role of MANETs for Healthcare Applications "Computer Science and Information Technology,Vol 1,Issue(2), Pages 73-81, 2013.

[11] Enji Sun, Xingkai Zhang, Zhongxue Li, "The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines" Safety Science,Vol 50 Pages 811–815,2012.

[12] T. A. Ramrekha, "Routing Challenges and Directions for Smart Objects in Future Internet of Things", IETF Smart Object Workshop, February 11, 2011.