



## **Security with Respect to MANET (Mobile Ad-hoc Network) and IoT(Internet of Things)**

**VIKRAM AGRAWAL \***

IT dept, BVM Engineering College, G.T.U. Gujarat, India.

\*Corresponding author E-mail: agrawal.vm@gmail.com

<http://dx.doi.org/10.13005/ojcs/10.01.11>

(Received: February 09, 2017; Accepted: March 03, 2017)

### **ABSTRACT**

MANET is self organizing, decentralized and dynamic network. In which participating nodes can move anywhere. The nodes can be host or router anytime<sup>1</sup>. Mobile ad hoc network is decentralized network so if one node is participating as router for particular time but if that node leave network then it is very difficult to transfer data packets. The main feature of MANET network of self organizing capability of node has advantage and disadvantage as well. By this it is easy to maintain network and convert topology but at same time we need to tolerate data transfer. The MANET is also used for big network and internet but there is no smart objects like IoT which can share information machine to machine. Now rapidly increase internet users worldwide to access global information and technology<sup>2</sup>. IoT is basically used to converge applications and services to open global business opportunities which can use I-GVC (Information-driven Global Value Chain) for efficient productivity.

**Keywords:** IoT, MANET, Global, Security.

### **INTRODUCTION**

Now six billions people around the world access internet by any of field area network like 2G, 3G, 4G, LTE, wifi, Wimax, Mobile Broadband, wired, etc.. They use the FAN for browsing the web, sending and receiving emails, accessing multimedia content, playing games, social networking and other tasks, so more peoples come to in connect to share global information and communication infrastructure. The one new leap is coming when we talk about IoT and internet as global platform. That is smart object communication, dialogue and self organizing devices. Allthe supporting

technology like MANET are used to recognize such model vision and put collectively properly applications and services knowledge to open new commerce opportunities. During deploying IoT with heterogeneous devices and network have to face privacy and security related problems so by using one implemented model as reference model of IoT, we can go towards our goals.

### **MANET has following system level features**

- Autonomous Nodes: Each moving node is an autonomous node, which may work as both a host and a router<sup>3</sup>.

- Distributed Operation: The nodes in MANET work together, where each of them acts as a transmitted node to implement functions<sup>4</sup>.
- Multi-hop Routing: When delivering data packets from a source to destination from one wireless network to other, the packets should be forwarded via one or more intermediate node<sup>5</sup>.
- Dynamic Network Topology: In MANET any node can move or enter any time without knowing neighbor nodes but the network can manage topology dynamically by own.
- Light-weight Terminal: The MANET nodes have less CPU processing capability, small memory size and low power storage.

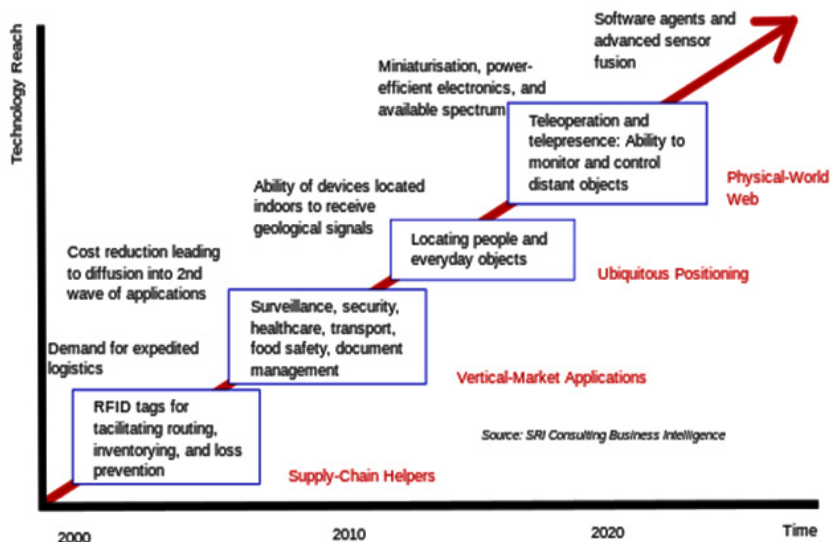
- Power is critical: it is same feature for MANET to concentrate. In IoT many applications needs to run for years over batteries and reduce the overall energy consumption.
- IoT's complexity: IoT application should be easily developed by any experts and use data from cloud or databases
- Real Time data management: there are many services which require to manage data real time and to deploy in application.
- Rich analytics & insights: smarter products come with insight understanding. IoT data talks back to your business with real time analytics.
- Cloud to cloud or DB to DB connectors: it is very difficult to manage all the information of global value chain of IoT in single cloud or Database so it is necessary to provide connectors which can help to exchange information or data of physical products.

**IOT should have following system level features**

- Sensing complex environment: innovative ways to sense and deliver information from the physical world to the database.
- Product identity management: IoT should identify products in cloud with the presence of internet. It should use flexible data store to customize dynamic data for any products with authorized applications and nodes
- Connectivity: the variety of wired and wireless connectivity is required to enable different application needs. For that first it requires to blur boundaries of countries.

**Technology Roadmap of IoT<sup>6</sup>**

Above diagram shows the technology roadmap of IoT. It covers RFID tag to software agent. That is roadmap for IoT in supply chain management. In this example the product and delivery of physical products all are involved to exchange information to gain single goal. The supply chain management share its data to vertical market applications like transport, food safety, document management, healthcare and



**Fig: Technology roadmap: The Internet of Things**

etc.... these all applications also have ability to get geographical position of people and objects. These share the location between each other. There is one more module which can monitor and control the distant objects.

### Security features at intersection of MANET and IoT

- Incorporation of secured MANET Routing Protocol in IoT: In MANET there are many protocols are available which provide better security in network but to manage security in IoT is challenging task because of heterogeneity of devices which are network together. So IoT are very bad to many attacks like malware, botnets, denial of services and many web based and android based malware. Therefore it is necessary to develop standard framework for IoT communication which can apply in heterogeneous environment.
- Security feature of IoT satisfying Confidentiality: The confidentiality means whatever the information are stored or exchanged is safe from unauthorized access or passive attack. Whatever the data are shared in IoT communication, are encrypted using well developed light weight algorithm.
- Secured Routing in MANETs and IoT: In MANET and IOT all packets are exchanged using hop to hop communication methods so cryptographic techniques are used to keep the routing information secured during transmission of packets. That is challenging work in IoT because there are many secure protocols are researched in MANET but IoT is just recent topic to implement.
- Design of secured communication scheme for IoT in MANET Environment?: we use MANET technology for particular area only but IoT is established to blur the boundaries of countries so for that to design secure communication scheme which can fit for IoT and MANET. For that we can develop some authentication system which can easily identify application, services, its location and end users.

- SON (Software OrganizingNetworking) Architecture for IoT<sup>8</sup>: the SDN technology is mainly used in wireless network because it is easy to maintain and just because of software definition, network can easily adopt topology runtime. The IoT is heterogeneous in network and in devices, so bandwidth consumption rate, transmission rate and delay rate are important statistic value to consider. An innovative multi-network architecture and controlling system is developed to decide a better performance metric in IoT network. The information and data coming from multi-network system can be stored and analyzed in single framework database or cloud. If multi-network architecture is established in efficiently way then it can be found improved throughput with large volume of data.

### CONCLUSION

Due to handshaking between and IoT, it can be achieved good interactive and communicative architecture of IoT. The MANET is already successfully run in our environment so with some minor changes and providing light weight cryptographic system, IoT achieve significant role in all services like traffic management, smart cities, smart building, controlling, monitoring, logistics etc..in this context complete analysis and research should be carried out because there is mainly two problem for integrating IoT.

1. **Technical:** technically implement IoT in any industry require massive amount of R&D. services will require multiple devices, sensors and actuators from suppliers to be exposed to developers. Only company with sufficient scale will understand technical issues and manage them.
2. **Financial:** In the emerging industrial structure will recoup enough money to reinvest in the R&D to capture value added services. The industries or stakeholders who do not take active part of integration system of information driven value added chain, they all produce inputs for system integrators at lower value chain.

## REFERENCES

1. Agrawal, Vikaram M., and Hiral Chauhan. "An Overview of security issues in Mobile Ad hoc Networks." *International Journal of Computer Engineering and Sciences* 1(1): 9-17, (2015).
2. Daniele Miorandi, Sabrina Sicari, Francesco DePellegrini, Imrich Chlamtac, "Internet of things: Vision, applications and research challenges", *Ad Hoc Networks*, 10, 1497-1516, (2012).
3. Vikram M. Agrawal, Samip A. Patel, "A STUDY ON SECURITY LEVEL OF AD HOC ROUTING PROTOCOL TO FIND OTHER APPROACH WITH DSDV", in *IJCET (IAEME)* 4(6), 240-246, (2013). ISSN 0976 - 6367(Print), ISSN 0976 - 6375(Online).
4. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," *Security Protocols*, 7th International Workshop, LNCS, Springer-Verlag, 2009.
5. Kuldeep Sharma, Neha Khandelwal and Prabhakar M., "An Overview Of security Problems in MANET," <http://psrcentre.org/images/extraimages/155.pdf>
6. A technology roadmap of the Internet of Things, 4 April 2008, Appendix F of Disruptive Technologies Global Trends 2025 page 1 Figure 15 (Background: The Internet of Things), SRI Consulting Business Intelligence/National Intelligence Council
7. Zhang Hua, Gao Fei, Wen Qiaoyan "A Password-Based Secure Communication Scheme in Battlefields for Internet of Things", *China Communications*, 8(1), 72-78, (2011).
8. Zhijing Qin, Denker, G., Giannelli C., Bellavista P. Venkatasubramanian, 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.