IOT Device Security Enhancement and Improvment

Er. Shailja Goyal, Er. Urvashi Garg
Student (M.Tech), Dept. of C.S.E, HCTM, Kurukshetra University, Haryana, India
Astt. Professor, Dept. of C.S.E, HCTM, Kurukshetra University, Haryana, India

ABSTRACT

IOT (Internet Of Things) are now a day's finding its place all over the fields related to the automation of different computer attached systems. These systems are smart enough to perform and decide the different control parameters according to the sensed value. The sensing value and the sensor security are the two key players in the IOT. As the advancement of the field it is being used in the applications like smart home, automated farm houses, smart environment control and so on. The error in data value can be the cause of the irregularity in the automation system as this automation is based on the sensor input. Along with the automation the security feature is also required for the IOT devices so that any of the attacker can't get control of the system. These sensors are performed with limited computational environment, these environment restrict the use of minimum rekeying of the devices for the security as the frequent rekeying results in the complete configuration to change and complete system update, this update may take some time and results in interruption of system services. The proposed scheme removes the data irregularities arising due to noise and also deploys the key exchange strategy to perform the system level security between the system and the devices.

Keyword : - *Iot Device, improvement , security, survey etc…*

I. Introduction

A growing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea of the Internet of Things (IoT). A basic example of such objects includes thermostats and HVAC (Heating, Ventilation, and Air Conditioning) monitoring and control systems that enable smart homes. There are also other domains and environments in which the IoT can play a remarkable role and improve the quality of our lives. These applications include transportation, healthcare, industrial automation, and emergency response to natural and man-made disasters where human decision making is difficult.

The IoT enables physical objects to see, hear, think and perform jobs by having them ―talk‖ together, to share information and to coordinate decisions. The IoT transforms these objects from being traditional to smart by exploiting its underlying technologies such as ubiquitous and pervasive computing, embedded devices, communication technologies, sensor networks, Internet protocols and applications. Smart objects along with their supposed tasks constitute domain specific applications (vertical markets) while ubiquitous computing and analytical services form application domain independent services (horizontal markets). Fig. 1 illustrates the overall concept of the IoT in which every domain specific application is interacting with domain independent services, whereas in each domain sensors and actuators communicate directly with each other.

Over time, the IoT is expected to have significant home and business applications, to contribute to the quality of life and to grow the world's economy. For example, smart-homes will enable their residents to automatically open their garage when reaching home, prepare their coffee, control climate control systems, TVs and other appliances. In order to realize this potential growth, emerging technologies and innovations, and service applications need to grow proportionally to match market demands and customer needs. Furthermore, devices need to be developed to fit customer requirements in terms of availability anywhere and anytime. Also, new protocols are required for communication compatibility between heterogeneous things (living things, vehicles, phones, appliances, goods, etc.).

Moreover, architecture standardization can be seen as a backbone for the IoT to create a competitive environment for companies to deliver quality products. In addition, the traditional Internet architecture needs to be revised to

match the IoT challenges. For example, the tremendous number of objects willing to connect to the Internet should be considered in many underlying protocols..

In 2010, the number of Internet connected objects had surpassed the earth's human population [1]. Therefore, utilizing a large addressing space (e.g., IPv6) becomes necessary to meet customer demands for smart objects. Security and privacy are other important requirements for the IoT due to the inherent heterogeneity of the Internet connected objects and the ability to monitor and control physical objects. Furthermore, management and monitoring of the IoT should take place to ensure the delivery of high-quality services to customers at an efficient cost.

The IOT architecture can be viewed as :

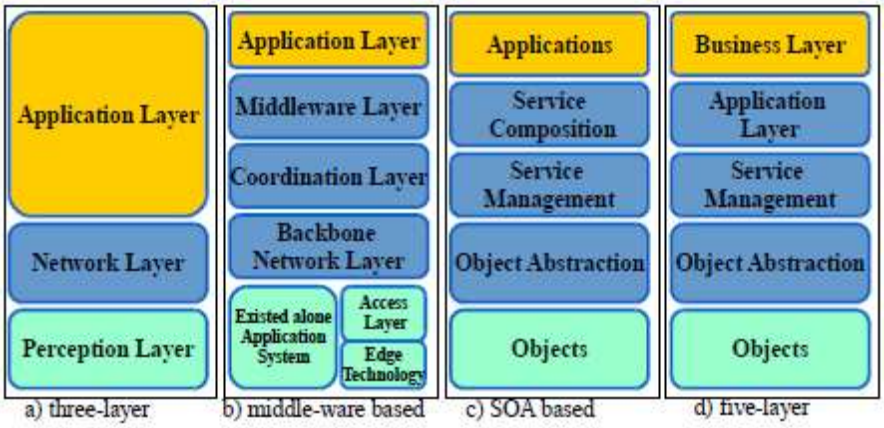

Fig 1: The IOT Architecture

II. Literature Survey

In [9], the author presents a novel architecture model for IoT with the help of Semantic Fusion Model (SFM). This architecture introduces the use of Smart Semantic framework to encapsulate the processed information from sensor networks. The smart embedded system is having semantic logic and semantic value based Information to make the system an intelligent system. This paper presents a discussion on Internet oriented applications, services, visual aspect and challenges for Internet of things using RFID, 6lowpan and sensor networks.

In [10], the author's study looks into the basic knowledge and privacy protection technology of Internet of things. The protection schemes mentioned above in the medical health care scene environment have been applied. The framework of the smart home system is proposed, and it implements the security privacy protection platform based on the design and realization of hardware and software, aimed at the security consideration.

In [11], the author not only describes about the evolution and how important of loT in daily life, the generic architecture, its most widely used protocols, numerous possible applications but also concern over security and privacy issues in loT, real-world implementation of loT system by using Arduino and its future trends. The loT probably becomes one of the most popular networking concepts that has the potential to bring out many benefits.

In [12], the author focuses to review the impact of some of the attacks attributable to internet of things. A desktop review of work done under this area, using the qualitative methodology was employed. This research may contribute towards a roadmap for security design and future research on internet of things scalability. The deployment of future applications around Internet of Things may receive valuable insight as the nature of attacks and their perceived impacts will be unveiled and possible solutions could be developed around them.

In [13], the author introduces the concept of application for internet of things and with the discussion of social and governance issues that arise as the future vision of internet of things. Further , description is given as IoT as envisioned is billion sensors connected to the internet through the sensors that would be generate large amount of data which need to analyzed, interpreted and utilized. Context aware capturing enables modeling, interpreting and storing of sensor data which is linked to appropriate context variable dynamically. Building or home automation, social smart communication for enhancement of quality of life, that could be considered as one of the application of IoT where the sensors, actuators and controllers can be connected to internet and controlled.

In [14], the author give an overview of some technical details that pertain to the IoT enabling technologies, protocols and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues to enable researchers and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities without having to go through RFCs and the standards specifications.

All nodes in a WSN communicate with each other by radio channel which is open and can be accessed by anyone in the same range. This makes a great challenge for security. In addition, WSN can be deployed in different environment depend on different applications. The entire network is affected by this environment condition. Moreover, due to unreliable channel and severe environment, there are much more packet loss and fault in WSN than traditional networks.

Data collected by sensors may contain sensitive information and should not be leaked to unauthorized devices. Further, encryption keys and information about sensors themselves (e.g., identity, location, etc.) must be protected to prevent eaves dropping and attacks based on traffic analysis. These challenges require measures that provide data confidentiality for sensor networks. Integrity is required to prevent adversaries from modifying sensor data, for example, with the purpose of injecting false readings and therefore affecting the response to the sensor readings.

Table 1 Constraints of WSNs.

Constraints	**Details**
Physical	Severe environment, limited resources of memory, energy and computation
Communication	Unreliable channels and limited bandwidth, collision and latency.

IV. Problem Overview

THE problem addressed is related to the data generated by sensor nodes along with the noise and error produced in the reception or communication of data. The data so generated if reaches to the final destination or the base station – can alter the results and the interpretation of the data changes and change is the objective set for the data in some cases due to this change is observed. The observance directly depend on the number of sensor nodes present in the sensing field in active state who are responsible for the generation of data for the base station. The error value thus received if differ slightly from other values can be ignored because the deviation generated by these error values are not so high but if the difference is larger it can deviate to a large extent. For this along with the efficient scheme for the network communication the data fusion scheme is also used in the network for this it combines the two goals of coverage and efficiency as such.

A. *Description of the Work:*

- Data Gathering: (Observe) Data collection phase, how the data results collected.
- Signal Processing: (Observe) Preprocessing data – allocation done before the fusion process begins.
- Object Assessment: (Orient) after preprocessing it leads to => patterns and features (mean, median), these data are assigned to objects to generate the supporting values.
- Situation Assessment: (Orient) it involve the situation predictions, the data fusion process and analysis of results.
- Threat Assessment: (Orient) possible threat identification.
- Decision Making: (Decide): by system, separation of supported and deletion or removal of unsupported data.
- Action Implementation: (Act): Threshold application(d) => actual plan extraction

B. Pseudo Code:

The basic and the core data fusion strategy lies in between the removal of unsupported data from the collected values. This phase-and error removal for the proposed work can be given as:

The data fusion is done on the basis of similarity between data values. Error makes the sudden change in data or makes unsupported data. By unsupportive, it gives the ability to remove the sudden raises or fall in data. There is the importance of each value generated from the sensor node while maintaining the support levels. Functions are designed to separate out the supportive data from unsupportive and most generalized can be shown as:

For necessary support criteria:

1. support(a,b) € [0,1]
2. support(a,b) = support(b,a)
3. If |a-b| <|x-y| => support (a, b) > support(x, y) provided that x, y are greater than 0.
4. On the basis of above

$$\text{support}(a,b) = \begin{cases} K & |a-b| <= d,\ (K>0,\ d>0) \\ 0 & |a-b| > d \end{cases}$$

Pseudo code for the data fusion process:-

1. Size of Data - no. of sensing nodes responsible for the generation of sensing values.
2. Threshold – the sensing data get difference above which treated as a unsupportive value.
3. Sorting the (Data generated)
4. Refinement of Data may include deletion from most values.
5. Preprocessing of refined data.
6. Median and mean value for the data is generated.
7. Median value generation results in support value.
8. Mean value generate a separate support value.
9. Support value generated is compared.
10. Result is generated by the weighted result.
11. Step 1 to 10 is repeated in each phase of the data communication so that the data which reach to the base station is completely processed.

III. Results

The Results obtained by the experiments performed can be summarized as:

- Energy dissipation takes place around 40% of the compared algorithm. The energy dissipation decrease enables the network to continue with large number of nodes with the network and increases the stability time of the network. This increase further reflected.
- Packets to BS in case of Base paper ranges from 62% to 0% of the number of nodes present in the network while in case of proposed algorithm this percentage is modified and achieved at max 32% to 0%.
- Number of alive nodes takes the 19.57% of the network life time from first node dead to last node dead in the network while in case of proposed work it takes 77.48% of the network life time of the network..
- Number of cluster head max. percentage observed in case of base paper is 39% around while it is reduced by the proposed algorithm to 25% at maximum value.Cluster heads are elected randomly as in the traditional Base Paper protocol.

A. Convergence and Mean Square Error

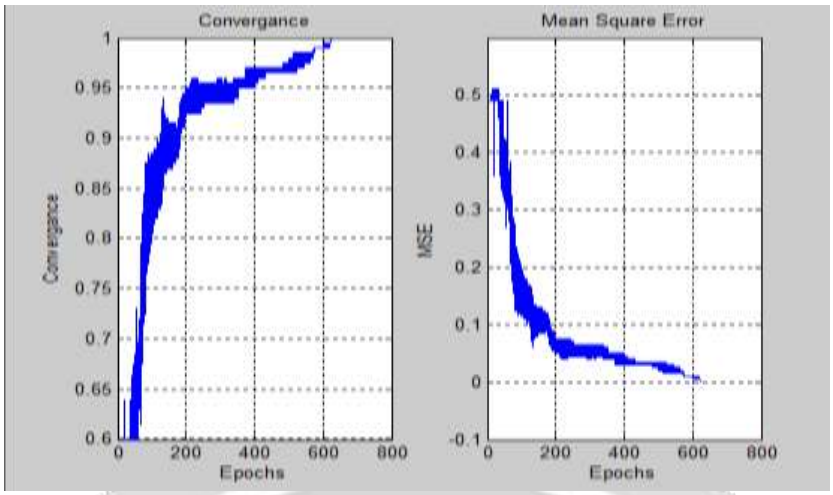

Fig 2 Plot for Mean Square Error and Convergence

This plot is done on the data generated as a result of the data fusion process, while this provides the information about the deviation observered from the actual value it also work as a measure of the correctness for the system.

IV. Conclusion

In the emerging new field of the IOT, each of the advancement comes with the various advantages and along with these advantages there may be some pitfalls which can be found and overcome be the extensive research. Present study takes two main criteria of data originality and data security which is from any other external agent as well as the internal error. These errors removed makes the system more reliable and secure to perform the automation task better to come with the new solution.

Simulation and the experimentation results for the IOT devices are plotted and the summarization of these results ensure to have the greater efficient and reliable network for the data reliability and energy efficiency. The data fusion task separates the unrelivant data generated by the IOT devices from being on the base station. Sensing data so collected, processed, filtered and forwarded to the base station contains the supported values. Supported values can be generated through various support function , for the mean and median method and further the fuzzy mean median method can be utilized along with the method supporting minimum deviation and error in support value generation. The threshold hold a greater degree of control for the inclusion of the values arriving near to unsupportive. The data error so removed , removes the possibility of error or attack in the form of false data packets or modified data packet thus, increasing the reliability of the system. This approach is carried out in the presence of Transfaulty nodes for the complete system implementation.

The proposed algorithm has shown a significant improvement over the studied protocol and taken as the base for the work undertaken. The difference among existing protocols and proposed algorithm include proposed algorithm keep track of the Energy consumption and the coverage in the network and the selection is done to have the best results for the given scenario. As the network time increses the coverage and the transmissions provided by the network are among the cases which covers the maximum space and area and provide the all direction network optimization.

.

References

[1] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO White Paper*, 2011.

[2] L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, pp. 2787-2805, 2010.

[3] R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in *Frontiers of Information Technology (FIT), 2012 10th International Conference On*, 2012, pp. 257-260.

[4] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Comput. Syst.*, vol. 29, pp. 1645-1660, 2013.
[5] P. Lopez, D. Fernandez, A. J. Jara and A. F. Skarmeta, "Survey of internet of things technologies for clinical environments," in *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference On*, 2013, pp. 1349-1354.
[6] D. Yang, F. Liu and Y. Liang, "A survey of the internet of things," in *Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010)*, 2010, pp. 358-366.
[7] Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *Communications Magazine, IEEE*, vol. 49, pp. 58-67, 2011.
[8] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," *Wireless Communications, IEEE*, vol. 20, pp. 91-98, 2013.
[9] Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-of-Things: Future vision, architecture, challenges and services." *Internet of things (WF-IoT), 2014 IEEE world forum on*. IEEE, 2014.
[10] Tian, Cuihua, et al. "Analysis and design of security in Internet of things."*2015 8th International Conference on Biomedical Engineering and Informatics (BMEI)*. IEEE, 2015.
[11] Kraijak, Surapon, and Panwit Tuwanut. "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends." *2015 IEEE 16th International Conference on Communication Technology (ICCT)*. IEEE, 2015.
[12] Gamundani, Attlee M. "An impact review on internet of things attacks." *Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on*. IEEE, 2015.
[13] Asghar, Mohsen Hallaj, Atul Negi, and Nasibeh Mohammadzadeh. "Principle application and vision in Internet of Things (IoT)." *Computing, Communication & Automation (ICCCA), 2015 International Conference on*. IEEE, 2015.
[14] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." *IEEE Communications Surveys & Tutorials* 17.4 (2015): 2347-2376.
[15] Kirichek Ruslan, Vyacheslay Kulik, and Andrey Koucheryavy. "False clouds for Internet of Things and methods of protection." 2016 *18th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2016.
[16] "Cc2420 data sheet." [Online]. Available: http://www.stanford.edu/class/cs244e/papers/cc2420.pdf
[17] "Telosb data sheet." [Online]. Available: http://www.xbow.com/Products/ Product pdf les/Wireless pdf/TelosB Datasheet.pdf
[18] Y. T. Hou, Y. Shi and H. D. Sherali, "On energy Provisioning and Relay Node Placement for Wireless Sensor networks" IEEE Transactions on Wireless Communications, Vol. 4, Mo. 5, pp.2579-2590, September 2005.
[19] M MIslaml, M A Matin2, T K Mondol l "Extended StableElection Protocol (SEP) for Threelevel Hierarchical ClusteredHeterogeneous WSN", (IEEE),vol: 5, pp. l -4, June 2012.
[20] ReetikaMunjal, Bhavneesh Malik "Approach for Improvement in LEACH Protocol for Wireless Sensor Network", Second International Conference on Advanced Computing & Communication Technologies (IEEE), pp.517-521, Jan. 2012.
[21] B.A. Sabarish, R. Lavanya,"Modified Leach Protocol for WSN", International Journal of Computer Applications, vol:-62, pp:-1-4, 2013.
[22] Shuo Shi, Xinning Liu and XuemaiGu "An Energy-Efficiency Optimized LEACH-C for Wireless Sensor Networks",7th International ICST Conference on Communications and Networking in China (CHINACOM) (IEEE) , vol:5, pp: 487-492, Aug. 2012.
[23] Smaragdakis. Georgios. Ibrahim Matta. AndAzerBestavros. "SEP: A stable election protocol for clustered heterogeneous wireless sensor networks", Boston University Computer Science Department, pp: 223-230, 2004.
[24] Thu Ngo Quynh l , Kieu-Ha Phung2,3, Hoan Vu Quocl, "Improvement of Energy Consumption and Load Balance for LEACH in Wireless Sensors Networks", published by:(IEEE), vol:73, pp.583-588, Oct. 2012.
[25] VivekKatiyar, Narottam Chand, Gopal Chand Gautam,Anil Kumar "Improvement in LEACH Protocol for Large-scale Wireless Sensor Networks",(IEEE), vol:32, pp:-1070-1075, Mar. 2011.
[26] Yuhua Liu Yongfeng Zhao Jingju Gao "A New Clustering Mechanism Based On LEACH Protocol", International Joint Conference on Artificial Intelligence (IEEE), Hainan, pp.715-718, April 2009.
[27] Shijun He, Yanyan Dai, Ruyan, "A Clustering Protocol for Energy Balance of WSN based on Genetic Clustering Algorithm", International Conference on Future Supported Education, pp:-788-793, 2012.