A survey of Trust Management in WSNs, Internet of Things and Future Internet

Kai-Di Chang and Jiann-Liang Chen
Department of Electrical Engineering, National Taiwan University of Science and Technology
Taiwan, R.O.C.
[e-mail: {d9807502,Lchen}@mail.ntust.edu.tw]
*Corresponding author: Jiann-Liang Chen

Received September 19, 2011; revised November 29, 2011; accepted January 7, 2012; published January 31, 2012

Abstract

Nowadays, most researchers and manufacturers always pay attention on wireless sensor networks (WSNs) due to its potential applications in many regions such as military, industrial and civilian areas. WSNs are the basic components of Internet of Things (IoT) and the key to machine-to-machine communications and the future Internet. Also, the security is an essential element for deploying WSNs. Recently the concept of trust-based mechanism was proposed in WSNs such as traditional cryptographic and authentication mechanisms. However, there is lack a survey on trust management for WSNs, IoT even future Internet. In this paper, we discuss the concept and potential application areas of trust management for WSNs and IoT worlds. Furthermore, we survey different trust management issues (i.e., cluster, aggregation, reputation). Finally, future research directions with respect to trust management in WSNs and future IoT world are provided. We give not only simple WSNs for IoT environments but also a simulated bootstrap platform to provide the discussion of open challenges and solutions for deploying IoT in Future Internet.

Keywords: Wireless sensor networks, IoT, M2M, trust management, future Internet.

This research was partly funded by the National Science Council of the R.O.C. under grants NSC 99-2219-E-197-001, NSC 99-2219-E-197-002, NSC 100-2219-E-197-001 and NSC 100-2219-E-197-002..

DOI: 10.3837/tiis.2012.01.001

1. Introduction

In 1999, the concept of Internet of things (IoT) was first proposed by Auto-ID Center - the EPC (Electronic Product Code) [1] system, which is a representative scheme for earlier IoT techolongy development. The EPC system aims all physical objects to be connected by RFID through a unique EPC code that carried by the RFID tag. Japanese Researchers also proposed UID solution as earlier IoT prototype. The IoT concept [2][3][4][5] is extended rapidly because the application requirements and technology developments have changed form time to time. Currently, IoT definitions are proposed based on different technologies and points of view. Some researchers propose RIFD or EPC based solutions such as Thiesse [6]. Broll et al [7] propose the things' Pervasive Service Interaction and Vazquez et al [8] propose the integration solution between smart objects and mobile services. However, most researchers pay attention on specific application or special function [9]. For instance, the application regions are including IoT security [10][11], network operations management [12] and so on. The Future Internet Assembly (FIA) has been founded by the European Commission to support fundamental and systematic innovation in Europe for realization of the Future Internet [13].

According to various IoT related researches, we can gain a knowledge that the architecture for future IoT has not been specified instead it is only featured with some characteristics. Objects in IoT have unique identity and virtual personalities operating in smart spaces [14] through using smart interfaces to connect or communicate with social, cyber and exchange user contexts. Thus, the technologies of the IoT can effectively promote the integration of production and service management, the integration of the physical world, digital world and cyber world. Then, it is well known by many people that the communications in IoT have been mainly supported by the evolution of information processing and service capabilities within IT industries.

After emerging of Internet and mobile communication network, the IoT has been regarded as the third wave of information technology. In ITU report, they declare "Machine-to-Machine communications and Person-to-Computer communications will be extended to things." Thus, the IoT would be part of the internet 3.0 or future internet.

Nowadays, the traditional mobile communication network and Internet are the most popular and mainly used in information transmission among people. The wireless sensor networks (WSN) can be used to achieve short distance communication among the sensor nodes by constructing wireless networks in ad-hoc architecture [15]. However, the WSN in ad-hoc manners is not simply communicate with mobile communication network due to lacking of standardization in protocols and suitable sensing technology. The data from WSN is also hard to transmit in long distance because the limitation of WSN's physical features and transmission protocols. There will be many objects in IoT world. Currently, with the wide deployment of WSNs, the huge architecture of WSNs can be regards as a part

of IoT.

The rest part of this paper is organized as follows: We show the motivation of our work in section 2. Then we introduce the history and concept of Internet of Things and future Internet in section 3. In section 4, we discuss the potential application areas of trust management and the classification of trust management is given. Then, we survey different trust management issues for IoT and future internet in section 5. The future research areas of trust management are proposed in section 6. Finally, we construct a bootstrap simulated platform for IoT traffic analysis, summarize our contributions and conclude this paper in last section.

2. Motivation

In this section, we introduce and explain the motivation of this research. IoT related research and development depends on the progress, technologies' specifications and the improvement of the social understanding, knowledge, rules and laws in this world. Thus, the standard, reliability, and robustness are important concerns for IoT development. The standardized architecture is the foundation for all technologies. If there is lack of a definite architecture, applications and services will be difficult to develop and integrate.

An important role to consist IoT in futurenet internet is Wireless sensor networks (WSNs). WSNs are composed of autonomous sensors which can be used to monitor environment's conditions such as temperature, sound, vibration, pressure and motion. People always pay attention on WSNs due to the great potential applications in many areas such as military, industry and civilian. For instance, WSNs can be deployed in battlefield surveillance, battle damage assessment, and industrial process monitoring. Cryptographic and authentication mechanisms are widely used for ensuring the security in WSNs. Recently, the concept of "trust management" is proposed for WSNs since the cryptographic and authentication mechanisms cannot effectively detect and avoid the internal adversarial nodes' problem. If one node does not trust other node, the transmission can not start. [16]. The basic idea of trust management is to establish the trustworthiness between two individual nodes. Sensor nodes need to seek their trust for opinions when facing uncertainty or start communication with new nodes. WSNs can encounter all types of malicious misbehavior with trust management. Also, IoT object can communicate with other objects in future internet. The basic consist of IoT can be wide deployed WSNs. With the enhanced nodes, the IoT prototype can be constructed.

In IoT world, there are various objects, the secured data transmission and the confidentiality, integrity and availability of data between different node are very important. Thus, it's important to effectively utilize trust management. In this paper, the potential application areas of trust management (i.e., topology control, coverage, target tracking, localization, Internet of Things) are first discussed, such as shown in. Further, different trust management issues (i.e., cluster, aggregation, reputation) in WSNs are surveyed. Finally, we provide further research directions regarding trust management for WSNs and

future IoT worlds.

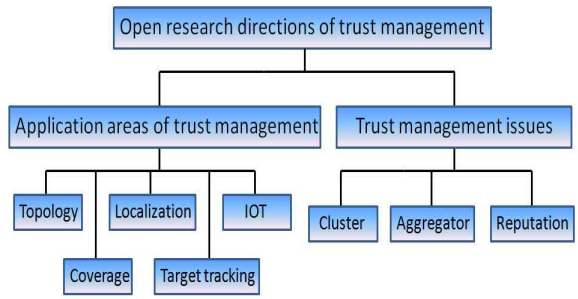

Fig. 1. Trust management in different Application areas of WSNs

3. Concept of IoT and Future Internet

3.1 Future Internet

In the future, people and objects will be connected anytime, anyplace, with anything, anyone, and appropriately utilizing any network and any service. The basic types of Future Internet are illustrated in **Table 1**, which is composed of IoT (Internet of Things), IoM (Internet of Media), IoS (Internet of Services) and IoE (Internet of Enterprises).

Table 1. Different type of IoX

Type	Basic Concept
IoT	Connecting wireless sensor network to mobile communication network and internet. The sensor nodes are regard as the "object/things" in IoT.
IoM	Connecting multimedia resources and applications in internet such as video or audio. As people known, there are many video platform such as youtube, PPStream, Justin.tv.
IoS	Operators deploy many services to users through internet. People can buy items on the internet, reading eBook through amazon, etc. There are many various services on the internet.
IoE	Enterprises start to complete their business achievement and process business related works on the internet. For instance, the business-to-business (B2B) electronic commerce and the

We can know the concept in Internet of anything in **Table 1**. As shown in **Table 1**, the Internet of Things is the most important part of Future Internet for providing a common global IT Platform to combine seamless networks and networked things over large-scale systems to cyber-physical systems [17].

3.2 Internet of Things

The Internet of Things (IoT) is regarded as new generation of information technology in communication networks and WSNs. It achieves more comprehensive service management through the internet or WSNs. The IoT architecture can be divided into three layers such as shown in **Fig. 2**. There are sensing layer, transmission layer, and application layer. In sensing layer, the IoT objects can collect data from physical world in sensor device, and then the data is transferred to the next layer through Bluetooth, RFID [18] or other technologies. In transmission layer, it is constructed based on the communication technologies to realize the integration of the perception and communication network, which receives data from sensing layer and combine with internet and WSNs forming IoT to physical world. In application layer, it is handled by corresponding management systems and then provided to all kinds of physical world users [19].

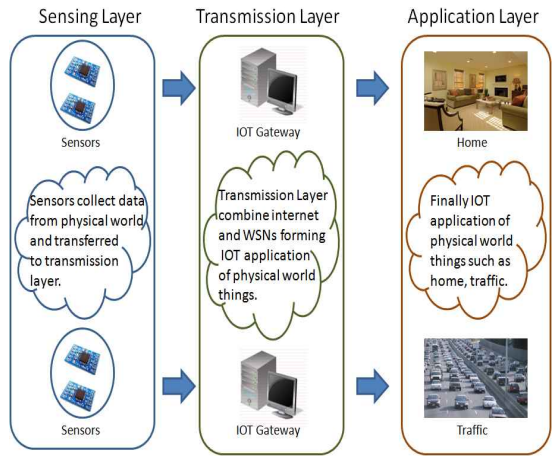

Fig. 2. Typical IOT application architecture

IoT combines a lot of technologies and includes many research fields such as network architecture design, sensor and object identification, information coding, data transmission, data processing, network planning and link/node discovery, etc. There are four key components of IoT:

1) Intelligent Sensors. Sensor node in traditional wireless sensor network was designed to sense data, store and forward the result to sink. In future internet IoT, the sensor node will embed more intelligent algorithms, cognitive capabilities. Thus, each sensor node would play the role of "intelligent object" instead of simple sensor node.

2) Data Aggregators. It is a moderate message processing which it should be designed to handle communicating messages.

3) Ubiquitous Network. Objects generate and communicate information physical conditions or item status when queries triggered. The network connectivity is always on to achieve information communication and data exchanging.

4) Context-Aware Services. This feature would enhance object's processing capability that will facilitate decisions to be made between devices without human intervention. Thus, the operations will be done automatically.

In addition to the four key components, there are three important characteristics in IoT:

1) Well Cognitive Capability - distributed sensing for Input / Output modules.
2) Robust Transmission - the robust and stable bus for industry communications.
3) Smart Process - programmable automation controller for adapting to variable data sensing environments.

In opinion of IoT, the three characteristics respond to four key components.

3.3 IoT Architecture

Ning and Wang proposed two IoT architectures [20] – Like Mankind Neural System and Social Organization Framework. Currently, the specification of IoT is not released and not well defined. There are also many researches discussed the possible IoT architecture. In our survey and opinion, the Ning & Wang's architecture considers WSNs, the concept of objects communication and data center. Thus, we regard their architecture as a possible IoT architecture.

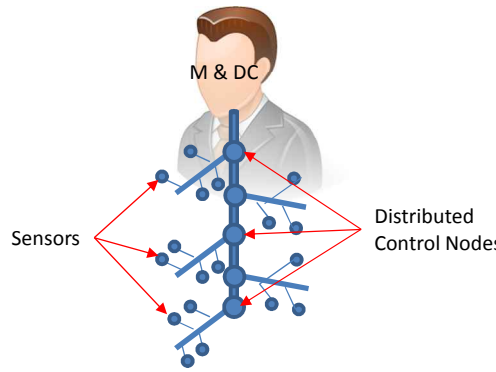

Fig. 3. Like Mankind Neural System

The Like Mankind Neural System (LMNS, as illustrated in) is consist of three components: 1) Brain - it responds for objects management and centralized data center, which is called M&DC, 2) Spinal cord - there are distributed control nodes for controlling lowest level sensors, and 3) A network of nerves - deploy IoT network and end-side sensors.

This architecture of IoT network transmits messages from low level sensors to the middle level control nodes and top level M&DC. It receives, translates, and sends back message to sensors to control the "things/objects." The M&DC is a centralized data center. It is in charge of processing information, storing data, and its most important task is to manage the IoT network.

In Ning's and Wang's design, the Social Organization Framework (SOF, as shown in **Fig. 4.**) plays three roles in IoT network. For national IoT, the SOF act as national management and data center which is called nM&DC. With these frameworks, the IoT object could

bring more computing power and capability to achieve high level calcuation.Thus, this framework can achieve more contribution to trust management for WSN.

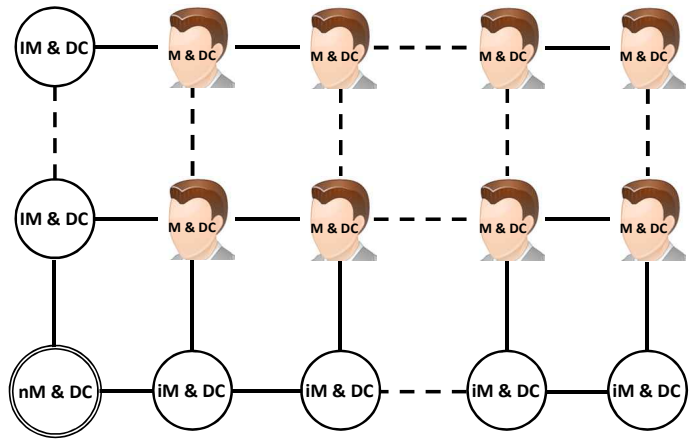

Fig. 4. Social Organization Framework

For IoT industry, SOF acts as industry management and data center which is called iM&DC. Finally, for regional IoT, SOF responds for local management and data center, which is called lM&DC. With different type of SOF IoT, each IoT has their achievements such as different level policy, monitoring, security, and backup of important data. The "Like Mankind Neural System" can be regard as single IoT network, then the "Social Organization Framework" is consist of many "Like Mankind Neural Systems" such as multi IoT networks. The major difference between LMNS and SOF is that each single IoT network can exchange information with other IoT network. It is like social network, one LMNS can share their sensors with different LMNS. The behavior and status is similar with human conversation in society. However, there is no traffic analysis or model for IoT on internet in their research and they do not mention about their IoT operation management in the two IoT architectures.

4. Trust Management Classification

There are various areas of trust mechanisms in wireless sensor networks that can be categorized in **Fig. 1**. The further descriptions are shown as follows:

4.1 Topology control

The main purpose of topology control is to assign and allocate transmission power. It is used to keep network connectivity and minimize power consumption as much as possible in order to avoid energy squander [21]. Topology control algorithms can be categorized into:

1) Deterministic algorithms: the current proposed method utilizes Simple Mobile Network (SMN) Model and Constant Rate Mobile Network (CRMN) model to incorporate mobility in topology control. The SMN model is a particular moving node with *n* static nodes. While CRMN model is *n* sensors that move around with every movement is associated with constant speed. The movement of each node can be represented by a line segment and keep network connectivity in every segment. Thus, the network can be connected during the entire movement period.

2) Non-deterministic algorithms: As for upper mobile network which consists of *n* moving nodes without specifying moving direction, it needs to consider distributed topology for stationary control. This mechanism is recomputed at the level of nodes' transmission power from the beginning of each interval based on their current location and any additional information about their movement. However, it is too difficult to choose suitable frequency to re-run the algorithm or select appropriate value for redundant transmission range [22].

4.2 Coverage

Coverage is a measurement indicator for showing sensed area in WSNs. It mainly affects network performance of WSNs such as localization or target tracking. In order to avoid sensor failures in initial deploying WSNs, we must consider environment condition due to external factor such as moist and scorching environment that will affect the measurement and eve sensor's lifetime. We consider two different methods to achieve this goal in order to set a preliminary deployment.

1) Self-deployment: It can mainly self-adjust position to improve sensor coverage deployment. The self-deployment in WSNs can be categorized as follows [23]:

Movement-assisted methods: The main idea is discovering the existence of coverage holes, and then calculates the target positions where sensors move to improve coverage.

Potential field methods: The potential field methods are usually used in mobile robotics to achieve local navigation, avoid to uneven terrain the obstacle influence, and can be also employed to achieve self-deployment.

Virtual force methods: These virtual force methods (VFM) sensors model can be regard as a combination of attractive and repulsive forces, and then use these forces to examine the coverage area.

2) Strategic relocation: In order to solve the relocation problem, Kong et al proposes strategic relocation solution. It uses Grid-Quorum technique to relocate redundant sensors to fill failed sensors' position to enhance its coverage [24].

4.3 Localization

The geographical information is an important data in WSNs. It will be difficult to manage sensors data without considering the node localization information. The localization algorithms can be divided into two categories [25].

Range-based: This is based on distance relative position. There are several typical examples for Range-based localization such as angle of arrival (AOA) – it utilizes point to

point arrival angle to estimate localization, Time of arrival of signal (TOA) - it utilizes signal point to point arrival time to achieve localization, and Time of difference of arrival of signal (TDOA) - it utilizes difference signal among of point to point arrival time to complete localization. All above examples have to be accomlished by utilization of point-to-point distance measurement. Although these methods can obtain high accuracy, there are still some defects can be found this method. It is often that the condition would be unacceptable because these methods need to use high cost devices or requiring careful environment profiling.

Range-free: Another method for achieving location information is Range-free. It does not depend on distance positioning because it does not directly measuring the distance. That can decrease the relative cost used in range-free approach. There are many positioning algorithms such as Amorphous Positioning, APIT and DV-Hop. Amorphous Positioning can achieve accurate positioning and tracking target through randomly placed this approach. APIT mainly performs broadcast mode and random position with low cost localization. DV-Hop will choose suitable signal node, divide them into groups, and then measure among of distance and position. **Fig. 2** shows the detail of comparison between range-based and range-free [26].

4.4 Target tracking

Target tracking mainly detects target sensors by measuring the energy of signals emitted from the targets. Then the performance metrics can be calculated by measuring probability of false (PF) and probability of detection (PD). The issues of target tracking can be categorized as following:

1) Mobility model: Establish target tracking data fusion model can effective collaborate between static and mobile sensors. An optimal sensor movement scheduling algorithm is proposed for minimizing the total moving distance of sensors in target detection [27].

2) Detection initiation: In order to efficiently use network resources for target tracking. The sensors have to be organized into local collaborative groups according to geographic information. Every group proceeds individual target tracking and coordinate their message transmission behavior [28].

3) Detection analysis: It defines sensor's upper bound delay and lower bound delay, utilizes sensors uncoordinated mobility and collaborative sensing at delay time, and then analyzes target sensor presence and absence [29].

5. Trust Management Issues in WSN

Mainly, there are three issues about trust management in WSNs – cluster, aggregation and reputation [30]. The details are explained as follows:

5.1 WSN Cluster

Cluster focuses on its nearby neighbor nodes; it chooses a cluster head from its neighbor coverage area. The nodes in cluster would listen and compute reputation to decide a sensor

node can be trusted or not.

The sensor nodes start pakcet transmission to a trusted node through infrastructure or ad-hoc mode. At this time, sensor node needs update and query other nodes' reputation; it can determine whether a neighbor node can be trusted or not in an appropriate time. This mechanism needs frequently aggreagte the data in order to complete trust management coordination. And with CKN or duty-cycle structure to manage power consumption, aggregation is frequently used to estimate sensors' trust structure because it could effectively discover other sensor nodes wheter it is illegal or misbehaving.

It can filter bogus data in the aggregation process, and convey cluster to determine other nodes' trust value. This mechanism is robust and does not require additional messages. Thus, it can reduce resource and energy consumptions in WSNs [31].

5.2 WSN Aggregation

In order to achieve transmission security, WSNs consider sensor nodes' trustworthiness. Thus, we need aggregation and calculate nodes' trust value within the clusters. Aggregation query is an effective mechanism to evaluate node's data and adapt to resource limitation in WSNs.

As long as node dispatches the messages, the aggregation process collects this information, and then compute it in other data section. The parent aggregate sensors transmit the data to children nodes, to determine the data is trusted or not and finally send it back to parent node. That means the cluster and aggregation distinguish illegal or misbehaving nodes through determining node with node among WSNs. We illustrate cluster scheme and data aggregation mechnaism in **Fig. 5**. The nodes in cluster are divided into a number of isolated aggregation sets. Each set evaluates trusted sensor nodes, report aggregation or opinion to cluster head, then cluster head responses to base station. In reverse opration, the base station queries cluster head, and then update data aggregation and reputation [32].

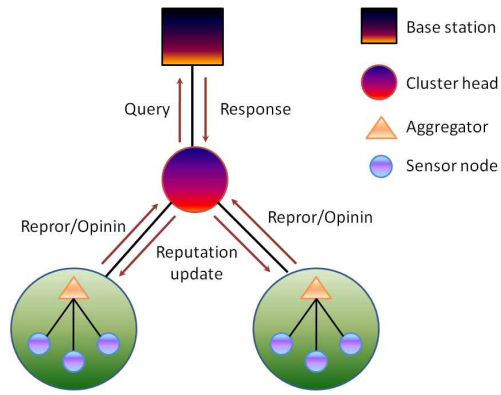

Fig. 5. Ideal schematic illustration of cluster and aggregation

5.3 WSNs Reputation

Reputation has been extensively studied and used within different technique. We introduce the details about reputation-Enabled for Target in WSNs.

The reputation scheme provides implement for detecting real environment. However, sensors measurement would lead system performance degradation, and causing the low network service quality low and resulting on huge power consumption. Supports from encryption for instance using disappeared message will make reputation system achieve positive outcome. However, it is still unsolved problem and this technique is not stable. Thus, the suggested sensing model should be mixed with Gaussian model for every node, and then use reputation parameters to the sensor model and modify nodes' measurement. The reputation is based on coordination with local voting algorithm to filter untrustworthy data enabling delivery packet to reach higher reliability and accuracy. Reputation is important in trust management and has been used in many purposes such as WSNs, ad-hoc, UWSN, simulator. Each reputation model would construct the whole system according to environment and conditions. For instance, Cobweb model differentiate traitor attacks [33], based RS (reputation system) construct SVM differentiate malicious nodes the accuracy [34]. These examples explain that each reputation constructions are based on current situation with different structure and reputation is important for trust management in WSNs.

6. Trust Management for IoT and Future Internet

According to our survey on current trust management in WSNs, we illustrate and suggest the future research direction as follows:

Application areas of trust management: In the WSNs, we have to consider various factor for trust management. Many researchers consider mobility in WSNs to dea with practical implementation. For considering mobility for WSNs, we need enbale the insider topology control such as deterministic algorithms and non-deterministic algorithms, deployment self-deployment and strategic relocation, target tracking mobility model, detection initiation and detection analysis, as well as multiple and stationary problems. The localization must be considered with positioning problem. That needs two algorithms (range-based and range-free) to choose for localization. Finally, we can achieve to goal of IoT according real implementatio requirement.

Trust management issue: Based on principles in trust management, there are many trust management methods with the similar principle. We summarized the most applied principles in trust management and detailed analysis them in this paper. The frequently utilized cluster or aggregation mechanisms can distinguish trusted and non-trusted sensors, control further transmission and coordination reputation mechanism, create IoT structure for further management trust data, and consider duty-cycle control energy consumption. Finally these mechanisms can efficiently solve problems through simulators.

We suggest future trust management research for WSNs according to above description. We must consider more parameters for each sensor node such as mobility, deployment localization, and indirect consider UWSNs security. Trust management uses reputation mechanism and combines with framework cluster, such as aggregation. For efficiently

managing physical world and considering users' convenience, the future IOT should help the internet and people to improve whole system. Table I shows our explored references in trust management for WSNs. We explore different mobility research in these WSNs paper for trust management, centralized/distributed, reputation, system model.

7. IoT Deployments and Traffic Analysis

7.1 Evaluation of IoT Deployment

In simulation environment, the main consideration of deploying IoT network is to connect lower layer of objects to the Internet. Thus, we use the OPNet network modeler to evaluate the IoT deployment, construct a bootstrap platform and map it with Ning and Wang's Like Mankind Neural System [20]. The component mapping is described in **Fig. 3**, the object model and bootstrap platform are given in **Fig. 6** and **Fig. 7**.

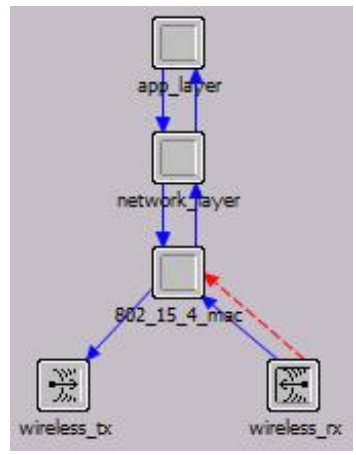

Fig. 6. Model for 802.15.4 based IoT Object

Table 2. IoT component mapping

In Ning and Wang's LMNS[20]	In our approach
M&DC	IoT Coordinator
Distributed Control Nodes	IoT Router
Sensors	IoT Object

Table 3. Simulation Parameters

Environment	
simulation time	300 seconds
range	100x100 meters
No. Coordinator	1
No. Router	4
No. Object	10
MAC Wait duration	0.05s
Number of Retransmissions	5
Miminum Backoff Exponent	3
Maximum Number of backoff	5
Channel Sensing Duration	0.1
Tranmission Bands	2.45G
Trnamit Power	0.05w
Packet Interarrival Time	1
Packet Size	1024bits

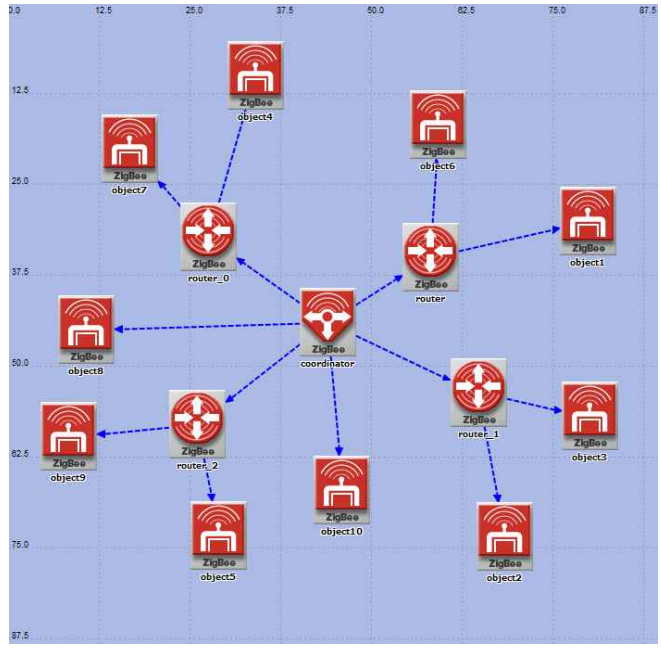

Fig. 7. IoT Bootstrap Platform Scenario

7.2 Traffic Analysis

In our simulation, each object will send 1024 bits packet per second, in order to store sensed information to coordinator in this IoT bootstrap platform. Then the coordinator handles those messages, feedback to each object. We measure number of hops, traffic to

coordinator, router and object, and finally the average end-to-end delay.

The number of hops for data transmission is shown in **Fig. 8**. Most objects send their data to coordinator by one hop. However, some data is delivered via more than 2 hops. The reasons are the native limitation of IoT router and the distance from object to coordinator. That cause the information should be delivererd through other objects.

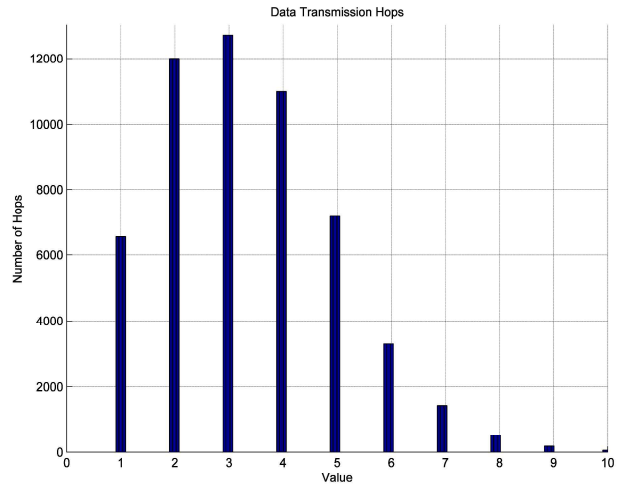

Fig. 8. Data transmission Hops

The traffic in bootstrap platform is drawn in **Fig. 9**. The IoT coordinator dominantly receives the data from objects. Here, the IoT router is merely forwards data from objects to coordinator.

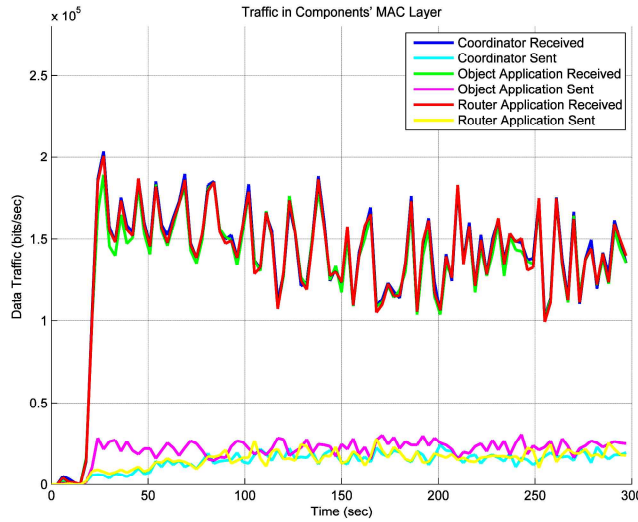

Fig. 9. Traffic in components' MAC layer

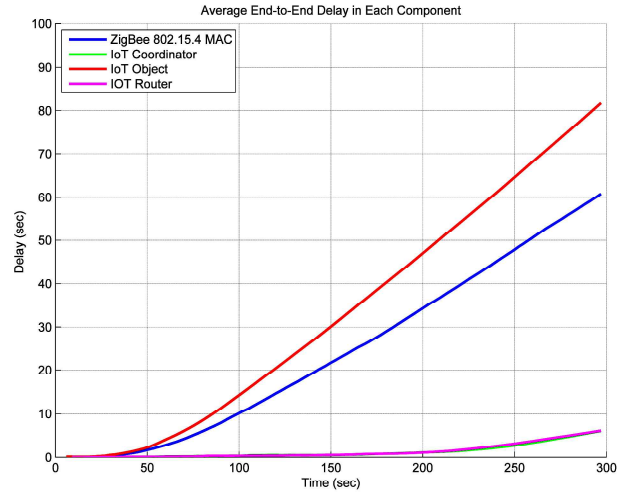

Fig. 10. Average end-to-delay in each component.

The average end-to-end delay is given in **Fig. 10**. In the beginning, the delay seems not very significant. However, when the traffic is increasing then the delay raises violently. The reason is that the queue length in each router and coordinator is fixed. Thus, the delay time grow with the continually incoming traffic.

6. Conclusion

Trust management has been an important research issue where many related mechanisms have been perviously proposed. However, different mechanisms should be implemented in different structures. Many theories are not consider some important factors such as trust management. In the paper, we introduce the application areas of trust management for IoT that based on topology, coverage area and target tracking. The trust management mechanisms such is applied, analyzed and dicussed in several aspects including cluster, aggregation, reputation. We provide future research directions for WSNs and future IoT. In addition we evaluated the IoT bootstrap platform using network simulator. We discover that the current Internet technology is insufficient to maintain the operation quality when constructing and deploying the IoT networks from traffic analysis results. In future research for WSNs and IoT, we suggest trust management should consider sensors topology, coverage deployment, target tracking, localization and IoT applications [35]. It also needs to consider cluster and aggregation structure that create reputation mechnism for the trust management in application area.

References

[1] EPCglobal, "The EPCglobal architecture framework," *final version 1.3*, 2009.
[2] J. P. Conti, "The Internet of things," *Communication Engineer*ing, vol. 4, pp. 20-25, 2006. Article (CrossRef Link)
[3] ITU, "The Internet of Things," *ITU International Reports*, 2005.
[4] "Internet of Things in 2020," *INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems Groups in co-operation with the RFID working Group of the EPoSS*, 2008.
[5] Qian Xiaocong and Zhang Jidong, "Study on the structure of "Internet of Things(IOT)" business operation support platform," *in Proc. of 2010 12th IEEE International Conference on Communication Technology (ICCT)*, pp. 1068-1071, Nov. 2010. Article (CrossRef Link)
[6] F. Thiesse, C. Floerkemeier, M. Harrison, F. Michahelles and C. Roduner, "Technology, standards, and real-world deployments of the EPC network," *IEEE Internet Computing*, vol. 13, pp. 36-43, Mar. 2009. Article (CrossRef Link)
[7] G. Broll, et al., "Perci: pervasive serviceinteraction with the Internet of things," *IEEE Internet Computing*, vol. 13, pp. 74-81, Dec. 2009. Article (CrossRef Link)
[8] J. I. Vazquez et al., "Communication architectures and experiences for web-connected physical smart objects," in *Proc.of 2010 IEEE International Conference on Pervasive Computing and Communications Workshops,* pp. 684-689, 2010. Article (CrossRef Link)
[9] L. Yan, Y. Zhang, Laurence, T. Yang, and H. Ning, "Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems," *Auerbach Publications*, 2008.
[10] E. Renault, "Toward a security model for the future network of information," in *Proc. of 4th International Conference on Ubiquitous Information Technologies & Applications*, Dec. 2009. Article (CrossRef Link)
[11] Liang Zhou and Han-Chieh Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Network*, vol. 25, pp. 35-40, 2011. Atricle (CrossRef Link)
[12] H. Ning, N. Ning, S. Qu, Y. Zhang, and H. Yang, "Layered structure and management in Internet of things," *Future Generation Communication and Networking,* vol. 2, pp. 386-389,

Dec. 2007. Article (CrossRef Link)
[13] Georgios Tselentis, Alex Galis, Anastasius Gavras, Srdjan Krco, Volkmar Lotz, Elena Simperl, Burkhard Stiller and Theodore Zahariadis, "Towards the future Internet-emerging trends from European research", *IOS Press*, 2010.
[14] Yun Wang and Kai Li, "Topology mining of sensor networks for smart home environments," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 7, no.3 pp. 163-173, 2011. Article (CrossRef Link)
[15] Huang Y. M., Hsieh M. Y., Chao H. C., Hung S. H. and Park J. H., "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 400-411, 2009. Article (CrossRef Link)
[16] S. Ganeriwal, Laura K. Balzano and Mani B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. of ACM Transactions on Sensor Networks (TOSN),* vol. 4, no.3, May. 2008. Article (CrossRef Link)
[17] Mo Jamshidi, "From large scale systems to cyber-physical systems," *Journal of Internet Technology*, vol. 12, no. 3, pp. 367-374, 2011.
[18] Yi-Wei Ma, Chin-Feng Lai, Chia-Cheng Hu, Ming-Chiao Chen and Yueh-Min Huang, "RFID-based seamless multimedia services for smart homes," *International Journal of Internet Protocol Technology*, vol. 4, no. 4, pp. 232-239, 2009. Article (CrossRef Link)
[19] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin, "IOT Gateway: bridging wireless sensor networks into Internet of things," in *Proc. of International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 347- 352, Dec. 2010. Article (CrossRef Link)
[20] Huansheng Ning and Ziou Wang, "Future Internet of things architecture: Like mankind neural system or social organization framework?," *IEEE Communications Letters*, vol. 15, pp. 461-463, 2011. Article (CrossRef Link)
[21] Y. Hong, K.-S. Lui and Y.-C. Wu, "HEA-Loc: A Robust localization algorithm for sensor networks of diversified topologies," in *Proc. of IEEE on Wireless Communications and Networking Conference (WCNC)*, pp.1-6, Apr. 2010. Article (CrossRef Link)
[22] C. Zhu, L. Shu, T. Hara, L. Wang and S. Nishio, "A survey on mobile sensor networks," *Osaka University, Technical Report,* Aug. 2010.
[23] M. Ma and Y. Yang, "Adaptive triangular deployment algorithm for unattended mobile sensor networks," *IEEE Transactions on Computers*, vol. 56, no. 7, pp. 946-847, Jul. 2007. Article (CrossRef Link)
[24] L. Kong, X. Liu, Z. Li and M.-Y Wu, "Automatic barrier coverage formation with mobile sensor networks," in *Proc. of IEEE International Conference on Communications (ICC),* pp. 1-5, May. 2010. Article (CrossRef Link)
[25] X. Xu, H. Jiang, L. Huang, H. Xu and M. Xiao, "A reputation – based revising scheme for localization in wireless sensor networks," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC),* pp. 1-6, 2010. Article (CrossRef Link)
[26] H. Chen, Y.T. Chan, H.V. Poor and K. Sezaki, "Range-free localization with the radical line," in *Proc. of IEEE International Conference on Communications (ICC),* pp. 1-5, May. 2010. Atricle (CrossRef Link)
[27] X. Zhang, "Decentralized sensor-coordination optimization for mobile multi-target tracking in wireless sensor networks," in *Proc. of IEEE Global Telecommunications Conference*, pp. 1-5, Dec. 2010. Article (CrossRef Link)
[28] W. Jin and Z. Xi, "Sensor self-organization for mobile multi–target tracking in decentralized wireless sensor networks," *IEEE Wireless Communications and Networking Conference*

(WCNC), pp. 1-6, Apr. 2010. Article (CrossRef Link)

[29] X. Wang, L. Ding and D. Bi, "Reputation-enabled self-modification for target sensing in wireless sensor networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 1, pp. 171-179, Jan. 2010. Article (CrossRef Link).

[30] M.C. Fernandez-Gago, R. Roman and J. Lopez, "A survey on the applicability of trust management systems for wireless sensor networks," *Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SECPerU*, pp. 25-30, Jul. 2007. Article (CrossRef Link)

[31] R.A. Shaikh, H. Jameel, B.J. d'Auriol, H. Lee, S. Lee and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698-1712, Nov. 2009. Article (CrossRef Link)

[32] H. Deng, G. Jin, K. Sun, R. Xu, M. Lyell and J.A. Luke, "Trust-aware in-network aggregation for wireless sensor networks," *IEEE Global Telecommunications Conference*, pp. 1-8, Dec. 2009. Article (CrossRef Link)

[33] S. Chen, Y. Zhang; P. Liu and J. Feng, "Coping with traitor attacks in reputation models for wireless sensor networks," *IEEE Global Telecommunications Conference*, pp. 1-6, Dec. 2010. Article (CrossRef Link)

[34] R. Akbani, T. Korkmaz and G. Raju, "A machine learning based reputation system for defending against malicious node behavior," *IEEE Global Telecommunications Conference*, pp. 1-5, Dec. 4 2008. Article (CrossRef Link)

[35] C.Y. Chen, H.C. Chao, T.Y. Wu, C.I Fan, J.L. Chen, Y.S. Chen, and J.M. Hsu, "IoT-IMS communication platform for future Internet," *Journal of Adaptive, Resilient and Autonomic Systems, IGI Global*, vol. 2, no. 4, 2011. Article (CrossRef Link)

Kai-Di Chang received his B.S. degree in electrical engineering from National Dong Hwa University, Taiwan, R.O.C. in 2007. He received his Master's degree in institute of computer science and information engineering at National I-Lan University, Taiwan, R.O.C. He is currently pursuing his Ph.D. degree in electrical engineering at National Taiwan University of Science and Technology. His research interests include VoIP, IP Multimedia Subsystem, Internet of Things and network security.

Jiann-Liang Chen received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering of National Dong Hwa University, where he is a professor and Vice Dean of Science and Engineering College. Prof. Chen joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a full professor now. His current research interests are directed at cellular mobility management, digital home network, telematics applications, cloud computing and RFID middleware design. Prof. Chen is an IEEE Senior Member and UK BCS Fellow. He has published more than 150 papers in journals and conferences, and also holds several patents.