Journal of Engineering and Applied Sciences 14 (2): 502-506, 2019
ISSN: 1816-949X

Secure Routing for IoT Base on Polling System

Seyed Mahmood Hashemi
College of Software Engineering, Beijing University of Technology, Beijing, China

Abstract: The Internet of Things (IoT) is the major elements of smart cities when we can see IoT devices in any points of our environment. There is need to special security policy to safe communication in IoT structure. In this study, we propose an approach to provide security in IoT communication. Proposed algorithm uses polling system to enable user's opinion about secure routing. The fuzzy system is used in this study to combine the votes.

Key words: Smart city, IoT, polling system, fuzzy system, major elements, devices

INTRODUCTION

Nowadays Internet of Things (IoT) affects on human life deeply. We can see IoT devices in any points of our environment. We can define IoT as a branch of information processing because we try to enact useful information via. IoT. Internet of Things (IoT) means all things that connect to internet and send/receive data. IoT is applicable in many fields:

Healthcare: The IoT can be used in health-care domain mostly. IoT remotely monitors patients, control drugs and track medical staff and equipment.

Industrial plants: IoT can be used to monitor and control different machines in an industrial environment for the formation of the final product (Hafiz and Johnson, 2009; Kondakci, 2015).

Military applications: In the military scope, IoT is used in a number of aspects that are harmful to humans such as the detection and intrusion of chemical, biological, radiations, explosive materials and acoustic signals. IoT architectures are also used for detection of mines in coastal chemicals and biological agents, the tracking of soldiers, the detection of snipers (Kumar and Singh, 2013; Vorster and Labschagne, 2005).

Rescue management systems: The major target of a rescue operation is to save the lives of people trapped in specific environments (generally dangerous environment) after natural or man-made disasters. IoT can support such activity as dissemination of details about the disaster Vorster and Labschagne, 2005).

However, IoT has many benefits for human lives, there is need to special security policy to safe communication in its structure. The major threat is about IoT assets. In this study, IoT assets are limited to medical devices that help doctors to remote monitor patients. Communication of medical devices need to confidentiality (to ensure send/receive data between doctor and patient) integrity (to ensure send/receive data is accurate) and availability (to ensue any times doctor and patient can communicate). In this study, we propose a structure base on polling system. Proposed approach has two benefits: firstly, it use user opinions, so, it is resistant in front of sudden changes, secondly, the interface of proposed system is completely understandable, so, users can be work with it very easily.

Literature review: Allocation proper bandwidth is challenged concept in secure routing. The elastic optical networks can provide bandwidth allocation to each connection request properly with using OFDM (Orthogonal Frequency Division Multiplexing) technology. The elastic optimal network method is flexible, so, it gets high spectrum utilization. The elastic optical network divides the high-speed data stream into orthogonal low-speed slots. Xuan *et al.* provides a static scheme for routing and spectrum assignment problem (Bottino, 2006). Researchers stablish an optimization model. Proposed model has two phases and in each phase it optimize just one object. According to their research, there are two objects with tree constraints to establish a connection. This routing method wants to minimize the maximum index of used slots and minimize the ration of blocked resources with constraints: the index of slots must be identical (consistency), a large connection request cannot be divided into several small connection requests (continuity), each slot should be assigned to one connection.

Actually hardware/energy consume of nodes is very important in secure routing. Unfortunately, previous works in this area cannot help us. For example, Yuan *et al.*

propose an algorithm which is called TSRAL, to rout data packets (Padyab *et al*., 2014). Proposed algorithm compare the measurement of all available path with a threshold metric and select best of them. This algorithm cannot be accepted because it static and also it considers all parameters in one formula and assign same weight to all parameters.

Since, wide rigorous network application, there is need a content-centric in front of host-centric. Mixia *et al*. (2007) describe the features of Information-Centric Mobile ad hoc Network (ICMNET) (Kbar, 2008).

Presented model must be powerful against attacks. Black hole Attack (BLA) is one kind of different attacks that affects data collection wireless networks. In this attack, adversary drops all data packets of an especial node that are routed, so, data cannot be usable or forward to the sink. In some researches to avoid BLA, data packet is divided into M shares which are sent to the sink via different routes. Unfortunately, this technique is energy consume. Another method is routing data packets is trust path, so, there is need to a trustable measurement. Obtaining the trust of a node is difficult and also is unclear.

Mixia *et al*. (2007) proposes a new method that active detection routing to address BLA. Their scheme has better energy efficiency than the previous ways. Proposed scheme has two stages: at first nodes with high trust are chosen and then secondly route along the successful detection. Although, their scheme considers energy consumption with high trusty routing but they suppose adversary is identified and also it is nodal.

Shen *et al*. depicts a scenario that individuals (objects) are in the Incompletely Predictable Network (IPN). It proposed a novel protocol named as Direction Density-based Secure Routing Protocol (DDSRP). In IPN, nodes are stable over a long period of time. Density is defined as similarity between coordinated destination and message transmitted. In proposed scheme, data-packets moving toward links with high density. Anand *et al*. propose a routing mechanism to ensure security in Mobile Ad hoc Network (MANET) (Hafiz and Johnson, 2009). There is no central authority in MANET. Each node performs routing role to route data packets from source to destination through the network. They have some limitations such as battery power ad bandwidth. researchers propose a scheme that creates a blend of both local and global reputation over a dynamic model. Actually, their research discusses about well behavior after node fail. Khan *et al*. uses MAC layer in mesh networks (Kondakci, 2015). In their approach information of two communicated hops are kept to increase security of routing. researchers consider two efficient parameters for their proposed mechanism: security and data-rate reduction. They use multi-hop in their scenario.

Although, security is considered in the routing protocols in wireless ad hoc networks and in the most of them is derived with extension of cryptographic and trust-based exiting routing protocols, secure routing problems are not solved in wireless ad hoc networks totally. Shcherba *et al*. propose an approach with using the flat rate trust levels, so, they enhance the flexibility. They use Dijkstra algorithm.

We can extract several parameters from previous research: number of slots (this parameter also presents density and reputation of information) cost (this parameter include energy/hardware, price etc which must be paid to transmit healthcare data) truthworthy.

MATERIALS AND METHODS

Preliminaries

Polling system: There is need for a system which can satisfy all stakeholder's opinion. We say stakeholder for anyone who has any role in developing a team. The polling system is an appropriate method for keeping votes (Breier and Hudec, 2011). The polling system consists of a source for the service and a number of queues for clients with a policy for assigning service to the client. For example in Fig. 1, λ_1, ..., λ_N are clients and S_1, ..., S_2 are assignment policies. The polling system can be a system with time sharing and N terminals. In that system, the central computer votes to terminals based on their requirements for data. Data transfers from terminals to the central computer through a voting scheme. Default:

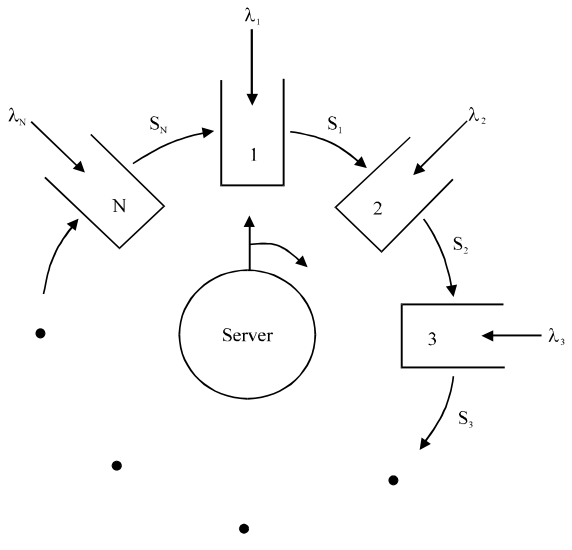

Fig. 1: Polling system

- Processes enter into the queues with a Poisson distribution
- Clients are served during the time as a random variable
- After servicing to a queue, the server assigns to other queues with a switch-over time (Viehmann, 2012)

Common polling systems are (Wang, 1997; Feng *et al*., 2014):

Exhausted: Server is assigned to a queue for all clients in that queue.

Gated: Server is assigned to a queue with a specific time range.

Limited-1: Predefined clients which can give server. Polling system has various applications.

Token ring networks: In a cyclic net, terminals need acceptance of the central computer (Hafiz and Johnson, 2009).

Robotic systems: A robotic system consists of a central robot and various inputs. For modeling this system, we can use the polling system where the robot is the server and the inputs are clients. Clients are set in queues based on their types.

Various non-generic computers and communication systems: In these systems, one processor serves to a particular type of task. A common way is to accumulate tasks into different types. In the model, tasks are clients and the processor is the server (Kumar and Singh, 2013; Viehmann, 2012).

Transportation (automated guide vehicle): In these models, many vehicles must be carried in a narrow way. The polling system consists of automated vehicles with default paths. In this model, transportation transforms clients from various queues to specific destinations (Breier and Hudec, 2011).

Stochastic Economic Lot Scheduling Problem (SELSP): This application is about producing by using a machine with limited capacity where the requirements produce stochastic (Viehmann, 2012; Wang, 1997).

Health care: An emergency in a hospital can be modeled with a polling system. Tasks are set in queues with an unlimited buffer.

Random polling: The best examples for these models are distributed control systems. There is no central control, so, deciding about the next terminal is done with polling.

There are some notes in the polling systems: Stability, priority, structure for polling, definition of limitations and waiting time.

Fuzzy logic: Fuzzy systems are knowledge-based systems or rule-based systems (Silva *et al*., 2014). Fuzzy system consist the number of rules. Each rule relates input (s) to output (s). Input (s) and output (s) in fuzzy system are recognized in fuzzy sets.

Let a system with uncertainty have the input output relation $y = fs(x)$ where $y \in R$ and $y \in R^{nX}$. A fuzzy system represents the knowledge related to inputs and output by nC fuzzy rules R_1, ... R_C which are expressed in the form R_i: If $(x_{k\ 1}$ isr $A_{i,1})$ and ,..., and $(x_{kn}X$ isr $A_{i,n}X)$ then $(y^*_{k,1}$ isr $B_i)$.

Where, $y_k = f_s(xk)$ is an observation vector (xk, yk) of the system, $x_{k,j}$ is the jth variable of x_k, $A_{i,j}$ is the membership function of the fuzzy set for the jth variable in the i'th rule which determines a fuzzy number for the j'th variable of input space, $y^*_{k,i}$ is the estimate of $y_k = f_s(x_k)$ by R_i, the operator "and" denotes the t-norm operation between two membership values and "Isr" denotes the belonging of an object into a fuzzy set.

An important contribution of fuzzy systems theory is that it provides a systematic procedure for transforming a knowledge base into a non-linear mapping.

The objective of non-linear mapping is producing output (s) with input (s). Mapping is done when there is a relation. Producing a relation (formula) from rules is role of inference engine. Researchers propose many inference engines and each of them has own features (strength/weakness).

RESULTS AND DISCUSSION

Proposed algorithm: The big problem for IoT is providing security for communications. The common approaches have two main weaknesses: firstly, they focused on the network analysis, attack modeling and etc and we do not have the significant approaches that consider the users opinions. Secondly, the presented approaches are understandable just for experts and they are sophisticated for ordinary users, the presented approaches cannot confident normal users. In contrast of them the proposed algorithm has two major characteristics: firstly, it works with stakeholders opinions and secondly it is user-friendly completely.

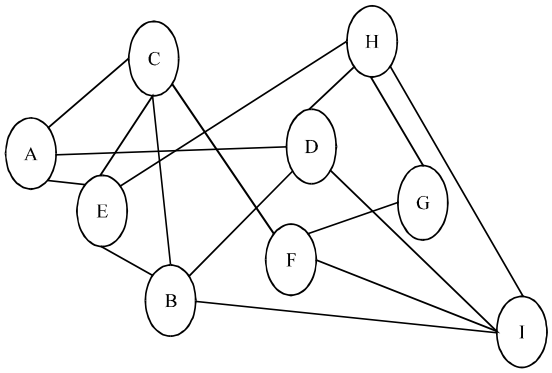

Fig. 2: Network

Proposed algorithm has two parts. The first part is gathering the votes and the second part is determine the security value. Let, there is a graph for modeling the network. The graph has N nodes and E links between nodes. We denote nodes with its label and denote the links with labels on their head (Fig. 2).

Graph is bidirectional. The objective of problem is secure routing. In other words, the objective is finding a path between source node and destination node which that satisfying the measurement of security. The measurements of security are confidentiality integrity and availability. Each links in the graph has three different weights that represent security values. However, the security measurements are qualified and not quantified, fuzzy system allows us to convert these values to special numbers. We propose our approach for medicine devices but it can be extents to other applications.

When one send/receive a data packet from source to destination, stakeholders have different opinions about secure routing. The first step of proposed algorithm is using a polling system to gathering the stakeholder's opinions. This polling system is represented in Fig. 3. Stakeholders (such as experts, users and etc) votes via. queues (which are denoted with Q_1-Q_4).

The next step is combine votes then convert it into a value. Algorithm uses fuzzy system. The heart of fuzzy system is inference engine. There is a variety set of inference engine types. In this study, we use product formula as inference engine. There is also need to definition of some fuzzy sets for input/output values of fuzzy system. We define three fuzzy sets for input and also five fuzzy sets for output (Fig. 4 and 5).

Let a data packet from node "A" send to node "I" (according to graphic scheme of network) and there are 8 stakeholders which vote to the paths. Votes are represented in Table 1.

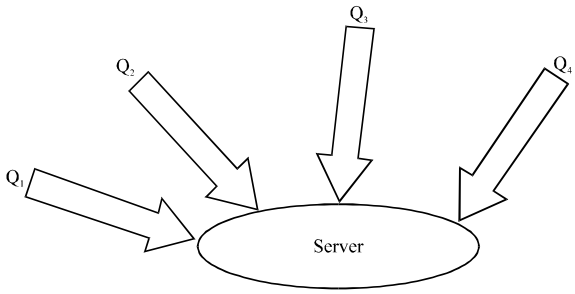

Fig. 3: Polling system in proposed algorithm

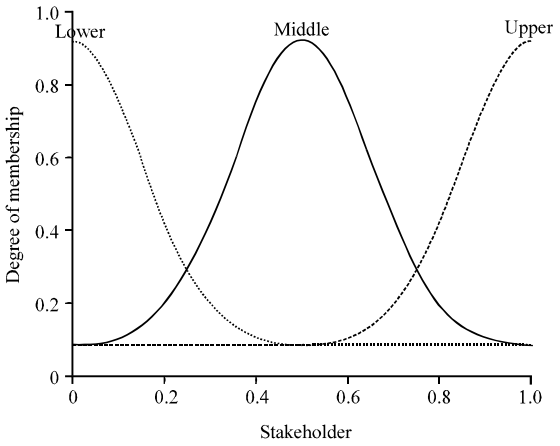

Fig. 4: Fuzzy sets for inputs

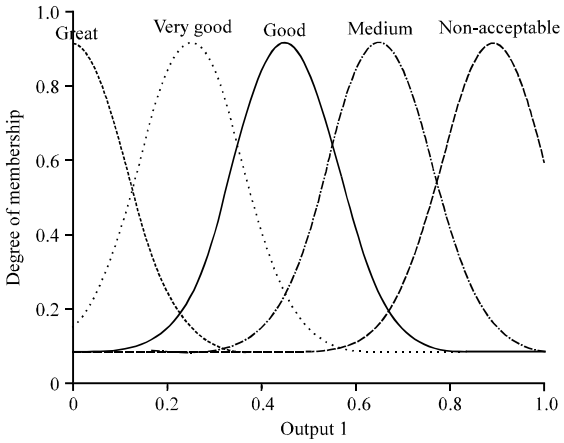

Fig. 5: Fuzzy sets for outputs

Table 1: Votes

Variables	Nodes
"Middle"	A, C, F, I
"Middle"	A, D, B, C, F, I
"Lower"	A, D, I
"Lower"	A, D, H, I
"Lower"	A, D, G, H, I
"Upper"	A, E, B, I
"Middle"	A, E, B, D, I
"Upper"	A, E, B, D, H, I

Stakeholders vote via. polling system and then their votes are evaluated with fuzzy system. The vote's stakeholders are entered to the fuzzy system base on fuzzy sets. Then fuzzy system decide result according to following rules.

Algorithm 1; Rules:

1. If (input1 is upper) and (input2 is unimportant) then (output1 is great) (1)
2. If (input1 is upper) and (input2 is normal) then (output1 is great) (1)
3. If (input1 is upper) and (input2 is normal) then (output1 is very_good) (1)
4. If (input1 is middle) and (input2 is vital) then (output1 is very_good) (1)
5. If (input1 is lower) and (input2 is important) then (output1 is medium) (1)
6. If (input1 is lower) and (input2 is vital) then (output1 is very_good) (1)

while the fuzzy system produces the results, we can select optimum of that

CONCLUSION

In this study, a new scheme for secure routing for IoT as the major elements of smart cities. Proposed scheme is based on fuzzy system. It means, we have to define numbers sets for 'Incipience' and 'Consequence'. Indeed, there is need to define some rules. Exact definition for incipience, consequence and rules cause proposed scheme specify and manage risks for computer systems carefully. Developers of computer systems can design and program components when there is an exact specification of security.

REFERENCES

Bottino, L.J., 2006. Security measures in a secure computer communications architecture. Proceedings of the 2006 IEEE/AIAA 25th International Conference on Digital Avionics Systems, October 15-19, 2006, IEEE, Portland, Oregon, ISBN:1-4244-0377-4, pp: 1-18.

Breier, J. and L. Hudec, 2011. Risk analysis supported by information security metrics. Proceedings of the12th International Conference on Computer Systems and Technologies, June 16-17, 2011, Vienna, Austria, pp: 393-398.

Feng, N., H.J. Wang and M. Li, 2014. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Inform. Sci., 256: 57-73.

Hafiz, M. and R.E. Johnson, 2009. Security-oriented program transformations. Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, April 13-15, 2009, ACM, Oak Ridge, Tennessee, USA., ISBN:978-1-60558-518-5, pp: 1-4.

Kbar, G., 2008. Security risk analysis for asset in relation to vulnerability, probability of threats and attacks. Proceedings of the 2008 International Conference on Innovations in Information Technology, December 16-18, 2008, IEEE, Al Ain, United Arab Emirates, ISBN:978-1-4244-3396-4, pp: 668-672.

Kondakci, S., 2015. Analysis of information security reliability: A tutorial. Reliab. Eng. Syst. Saf., 133: 275-299.

Kumar, R. and H. Singh, 2013. A qualitative analysis of effects of security risks on architecture of an information system. ACM. SIGSOFT. Software Eng. Notes, 38: 1-3.

Mixia, L., Y. Dongmei, Z. Qiuyu and Z. Honglei, 2007. Network security risk assessment and situation analysis. Proceedings of the 2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID), April 16-18, 2007, IEEE, Xiamen, China, ISBN:1-4244-1035-5, pp:448-452.

Padyab, A.M., T. Paivarinta and D. Harnesk, 2014. Genre-based assessment of information and knowledge security risks. Proceedings of the 2014 47th Hawaii International Conference on System Sciences, January 6-9, 2014, IEEE, Luleå, Sweden, ISBN:978-1-4799-2504-9, pp: 3442-3451.

Silva, M.M., A.P.H. De Gusmao, T. Poleto, L.C.E. Silva and A.P.C.S. Costa, 2014. A multidimensional approach to information security risk management using FMEA and fuzzy theory. Int. J. Inf. Manage., 34: 733-740.

Viehmann, J., 2012. Reusing risk analysis results--an extension for the coras risk analysis method. Proceedings of the Joint 2012 International Conference on Privacy, Security, Risk and Trust and Social Computing, September 3-5, 2012, IEEE, Amsterdam, Netherlands, ISBN:978-1-4673-5638-1, pp: 742-751.

Vorster, A. and L.E.S. Labuschagne, 2005. A framework for comparing different information security risk analysis methodologies. Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, September 20-22, 2005, South Africa, pp: 95-103.

Wang, L.X., 1997. A Course in Fuzzy System and Control. Prentice Hall, Upper Saddle River, New Jersey, USA., ISBN:9780135408827, pp: 424.