Journal of Engineering and Applied Sciences 14 (3): 951-959, 2019
ISSN: 1816-949X

LA-Based Approach for IoT Security

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

Abstract: The most important aspect in IoT is security. The provision of security in IoT systems is the responsibility of a trust management mechanism. However, a trust management mechanism comprises a number of components of which secure routing is vital among them. There are a number of effective parameters in secure routing which have been considered in the presented multi-objective optimization model. In this study, Multi-Objective Learning Automata (MOLA) was used to solve secure routing problem which can simultaneously optimize all parameters. There exist three methods of training LA and the results of the different methods were compared in this study. The proposed approach can be used with both administrator and users because their requirements are considered in a model and it is quite easy for administrator and users to comprehend.

Key words: Learning automata, multi-objective optimization, security, IoT, responsibility, parameters

INTRODUCTION

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 (Furtado and Trobec, 2011).

Industrial plants: IoT can be used to monitor and control different machines in an industrial environment for the formation of the final product (Palattella *et al*., 2013; Potter *et al*., 2013).

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 regions, the localization of modern diesel-electric submarines operating in littoral waters, the identification and localization of mortars, artillery and small fire arms, the measurement of trace concentrations of explosives, toxic chemicals and biological agents, the tracking of soldiers, the detection of snipers (Hussain and Sup, 2009; Durisic *et al*., 2012).

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 (Saha and Matsumoto, 2007).

As a coin with two sides, IoT has some disadvantages. The major blind spot which serve as a disadvantage of IoT is security. The IoT risks are exacerbated by the fact that having secure connection IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists have noted, companies entering the IoT market may not have experience in dealing with security issues. Second, although, some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable. Providing security for IoT system is the responsible of a Trust Management Mechanism (TMM).

The TMM must be used on every tasks of IoT (Fig. 1). In other words, TMM must check every request of service according to security policy. TMM comprises a number component such as secure routing, authentication, authorization, etc. The actual designing of TMM with acceptable degree of security is complicated but an easy method is presented here for TMM. The aim of this study is to present an approach for secure routing. The approach simultaneously optimizes multiple factors. Learning Automata (LA) is utilized in this approach. LA has a dynamic structure, hence, it can very well adapt to network circumstances. Indeed, the performances of LA will be compared with different methods.

Literature review: The researcher's contribution is divided into two sub-sections. Firstly, effective

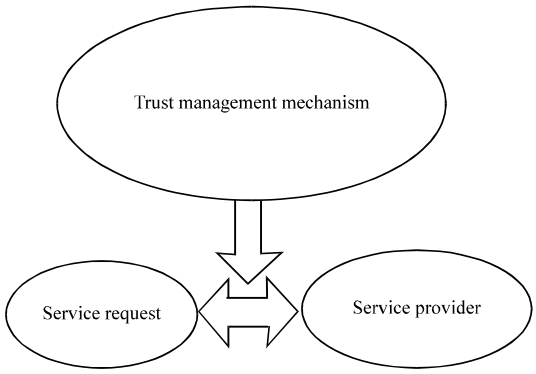

Fig. 1: Supervision of TMM

parameters and method are sought to be simultaneously optimized. Secondly, focus will be on using learning automata.

Effective parameters: Nehme *et al.* (2008) focused on three IoT requirements as the three key concepts of security: authentication, confidentiality and access control. These concepts are not absolute concepts for the security and can be diverse in other researches. It proposed the punctuation-based solution which has several advantages. First, the access control is dynamic and the speed of enforcement is fast because security restrictions are streamed together with the data. Second, the security punctuations may be shared by multiple tuples that have similar policies. Thus, no redundant copies of policies are stored, memory overhead is minimized and the security-related processing is shared. Policies in security punctuations can also be encoded in a bitmap format for compactness, thus, further reducing security-related processing. It is assumed that each query plan is associated with a per-unit-time cost, so, without this assumption, this research is not useful. Punctuation technique is used with other researches. Nehme *et al.* (2008) proposed stream security constraints called security punctuations. Security punctuations are meta-data introduced into a data stream to specify 'who' has right 'when' to stream 'which' data (Alcaide *et al.*, 2013). Actually, this research discusses about 'who' communicate and not about 'how'. The National Institute of Standards and Technology (NIST) defined incident handling as a whole lifecycle that includes the incident response (Rahman and Choo, 2015), so, it is upper reference for any research. Selecting countermeasures to security threats remains one of the most pressing issues that require attention on a continual basis. Each security strategy entails different costs, levels of effectiveness and potential benefits, many of these are difficult to quantify. Information security managers need to select security strategies on a periodic basis. A model that captures the complexities of the security decision while permitting the systematic exploration of alternative security decisions would be an invaluable aid to managers. Nazareth and Choi (2015) developed a model that permits information security managers to examine the effects of alternative security decisions on the organization's information assets but model is static and can not adopt to dynamic cirumstances. Ojamaa *et al.* (2008) utilized the metrics of the graded security method and built a model that relates security measures taken with the costs and confidences of achieving the goals. However, its model is well, the natures of cost and confidence are different, so compromise them into a formula is not logical. A fitness function that presents the integral confidence of achieving the security goals using one numeric value was introduced. Actually, security algorithms and protocols in traditional computer networks are hard to be directly applied for IoT. Li (2012) analyzed and discussed some keys and technical security issues in IoT. He designed three hierarchies in accordance to the network structure. The acquisition hierarchy is designed in such a way to realize an intelligent sense function, including information acquisition, capture and object identification, RFID, self-organized network, short-range wireless communication, low power router, etc. The major role of network hierarchy is to transmit and communicate information including the access layer and the core layer. The middleware hierarchy is mainly designed to realize the communication and function between network hierarchy and the application service of IoT. Since, the circumstances of network are divers randomly, this hierarchy may not be useful. RERUM stands on "REliable, Resilient and secUre IoT for sMart city applications" (Pohls *et al.*, 2014). The main goal of RERUM is to develop the reliability of IoT while providing privacy protection mechanism. Proposed mechanism does not consider all effective parameters in IoT. Abomhara and Koien (2014) focused on three issues: privacy for humans, confidentiality of business processes and 3rd-party dependability. According to them, security is an organized framework consisting of concepts, beliefs, principles, policies, procedures, techniques and measures required to protect individual system assets as well as the system as a whole against any deliberate or unintentional threat. Thus they try to compromise all parameters in one formula. According to the belief of Xu *et al.* (2014) hardware-based security is ideally addressed IoT security problems. They grouped IoT security desiderata into two classes: the first class is security tasks and the second class is related to design metrics such as cost, size, latency and in particular, energy requirements but their

method is hardware and can not be converted to software. Bose *et al.* (2015) focused on privacy in IoT systems. According to their claims, since, privacy is preserved with employing security mechanism over all collected data and it imposes considerable cost, then, resource optimized scheme for loT is of utmost importance in terms of both communication and computation cost optimization. Therefore, a novel contribution based on measured privacy is proposed. By Unger and Timmermann (2015) and Schurgot *et al.* (2015) proposed a hardware solution to address security and privacy.

In this study, we have two goals. First, we consider all effective parameters separately. Second, we present dynamic model, so, it can adopt to network circumstances completely.

Using Learning Automata (LA): One of the main uses of the IoT is in Vehicular Ad Hoc Networks (VANETs). There is an On Board Unit (OBU) in a VANET which helps with navigation, etc. Kumar *et al.* (2015) presented a new efficient decentralized Public Key Infrastructure (PKI) in VANETs using the concepts of the Bayesian Coalition Game (BCG) and Learning Automata (LA). LA can be used in many Intelligent Tutoring Systems (ITSs). Curilem *et al.* (2007), a new formalization of ITSs was presented. According to the researchers, the ITS is a system that models the behavior of a human tutor and he formalization of ITS is represented with automata theory. Ge *et al.* (2016) proposed a framework of IA with different LAs. Actually, the proposed method is dependent to its board.

A number of papers have tried to increase the ability of IA in learning. Krishna *et al.* (2013) proposed an LA-based algorithm, named LAVBA, to increase the performance of LA with minimization of the number of collisions. We can use this model. By Torkestani and Meybodi (2010), a Distributed Learning Automata (DLA) based backbone formation algorithm was proposed to alleviate the notorious broadcast storm problem by reducing the rebroadcasts. The aim of the proposed algorithm was to form a virtual backbone for the wireless ad hoc networks by finding a near-optimal solution to the minimum Connected Dominating Set (CDS) problem. This model can be presented in future papers.

MATERIALS AND METHODS

Preliminaries: This study briefly introduces a number of needed subjects. Firstly, the multi-objective optimization that is used in many fields is defined. Secondly, learning automata is defined as a tool for optimization with suitable results.

Multi-Objective Optimization (MOO): MOO is necessary when multiple cost functions are considered in the same problem. The aim of MOO is to tune the decision variables to satisfy all objective functions with optimum value. This class of problems is modeled by Eq. 1:

$$\begin{aligned} &\text{Optimize: } \left[F_1(X), ..., F_k(X)\right] \\ &\text{Subject to: } g_1(X), ..., g_m(X) \le 0 \\ &\qquad\qquad h_1(X), ..., h_p(X) = 0 \end{aligned} \tag{1}$$

Where:

k = The number of objective functions
X = The decision vector
m = The number of inequality constraints
p = The number of equality constraints

This goal causes a difference between these algorithms and their ancestor, single-objective optimization which is based on the concept of the best solution while MOO utilizes the concept of dominate solution. Dominance is defined by Unger and Timmermann (2015):

$$\vec{U} = (u_1, ..., u_n) \prec \vec{V} = (v_1, ..., v_n) \text{ if } \forall_i \in \{1, ..., n\} : u_i \le v_i;\ \exists j \in \{1, ..., n\} : u_j < v_j \tag{2}$$

In other words, a vector $\vec{U} = (u_1, ..., u_n)$ dominates another vector $\vec{V} = (v_1, ..., v_n)$ if and only if $\vec{U}$ can reach the optimal value for some criteria without causing a simultaneous non-optimal value for at least one criterion. If two vectors cannot dominate each other, they are called non-dominated vectors.

Learning Automata (LA): Automata can be represented by 5 tuples SA = {α, β, F, G, Θ} where α is a set of actions, β is a set of inputs of automata, F is a function that maps the input and current state to the next state $F \equiv \Theta \times \beta \to \Theta$, G is the output function that maps the current state to the next output and Θ is a set of states.

An automaton selects an action in α at each iteration. If the mapping of F and G is deterministic then the automata are called deterministic, otherwise, the automata are called stochastic. The output and next state of deterministic automata are achieved uniquely according to the initial state and inputs. For stochastic automata, just the probability of the output and next state can be determined. Stochastic automata are divided into two categories: fixed structure and variable structure. In fixed-structure stochastic automata, the probabilities of the next states and outputs are constant at the each iteration but in variable-structure stochastic automata they vary.

Learning algorithms can be divided into two categories: standard algorithms and model algorithms. In standard algorithms, the formula for learning is:

$$P(n+1) = T[P(n), \alpha(n), \beta(n)]$$

Where:

P = The probability of selection of an action
T = A learning algorithm which may be linear or non-linear

In other words, learning algorithms increase the probability of selection of action α_i and decrease the probability of selection of other actions if the desired response is received from the environment for action α_i at the n-th iteration. Otherwise, they decrease the probability of selection of α_i and increase the probability of selection of other actions. So, it can be said that:

$$\begin{aligned} P_i(n+1) &= P_i(n)+\sum_{\substack{i=1\\ j=i}}^{r} f_j\left[P_j(n)\right] \\ P_j(n+1) &= P_j(n)-f_j\left[P_j(n)\right];\ \forall_j:\ j\neq i \end{aligned} \tag{3}$$

For a desired response and:

$$\begin{aligned} P_j(n+1) &= P_j(n)-g_j\left[P_j(n)\right];\ \forall_j:\ j\neq i \\ P_i(n+1) &= P_i(n)+\sum_{\substack{i=1\\ j=i}}^{r} g_j\left[P_j(n)\right] \end{aligned} \tag{4}$$

For a non-desired response. Functions f are called the reward and penalty functions, respectively and r is the number of actions. In linear learning algorithms:

$$f_j\left[P_j(n)\right] = aP_j(n),\ 0<P_j(n),\ 0<\alpha<1 \tag{5}$$

$$g_i\left[P_j(n)\right] = \frac{b}{r-1}-bP_j(n),\ 0\le b\le 1 \tag{6}$$

There are three approaches for linear learning algorithms according to the different values of a and b:

$$\begin{aligned} &L_{RP}:\ a = b \\ &L_{RrP}:\ b \square\ a \\ &L_{RI}:\ b = 0 \end{aligned} \tag{7}$$

In the multi-objective expression, each solution may be one of three possible states. In the first state, a solution may dominate another solution (s). In this state, the probability of its selection is increased. In the second state, a solution may be dominated by another solution (s). Thus, its selection probability must be decreased. In the third state, a solution is non-dominated with another solution (s). The selection probability in the third state does not change.

Multi-Objective Learning Automata (MOLA) which can solve multi-objective problems is presented. The algorithm begins with the initialization of vectors. Number vectors (pop-size) are initialed randomly. Each one is a final solution potentially. After initialization, algorithm enters into a loop and this loop continues until the condition stops (max-iteration). At each iteration, three tasks are done.

Evaluation: all vectors are evaluated according to the cost matrix. Dominance decision: all vectors are compared to each other and base on the definition of Pareto dominance, their situation is decided. Each vector may be dominates another vector (s), dominated with another vector (s) or non-dominate with all vectors.

Learning: the probabilities of all vectors to select for next iteration are changed according to dominance decision. If any vector dominates another vector (s), its probability follows desire learning. If any vector is dominated with other vector (s), its probability follows non-desire learning. If any vector is non-dominated with other vector (s), its probability is not changed. The formula for desire learning is:

$$P_i(n+1) = P_i(n)+\left[a^*\sum_{\substack{j=1\\ j\neq i}}^{pop\text{-}size} P_j(n)\right] \tag{8}$$

The formula for non-desire learning is:

$$P_i(n+1) = P_i(n)+\left[\frac{b}{(pop\text{-}size-1)}*\sum_{\substack{j=1\\ j\neq i}}^{pop\text{-}size} P_j(n)\right] \tag{9}$$

Where:

$P_i(n+1)$ = The new probability
$P_i(n)$ = The old probability

Learning parameters are a, b and they are valued with three approaches: a = b, a » b and b = 0.

Proposed approach: This study comprises two sub-sections. Firstly, the environment is descripted. Secondly, problem is descripted and in the last sub-section the proposed algorithm is descripted.

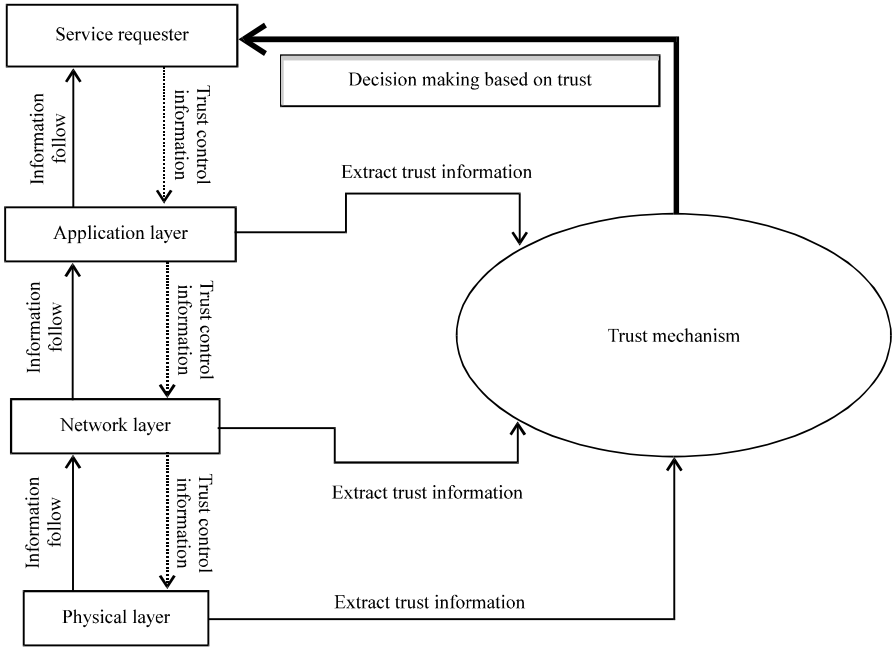

Fig. 2: Trust management mechanism

Environment: There exists a network with 10 nodes. Each node has a path to all nodes (they are recurrent). These assumptions do not eliminate generality. Each path has three characters: 'security', 'privacy' and 'cost'. Each of characters for paths ('security', 'privacy' and 'cost') may be either hardware or software. Hardware means electronic sensors receive information and software means experiments, interpretation of collected information, etc., we present network characters in which values are in [0, 1]. Characters values are random and present different level for each character.

Problem: IoT uses the network to transmit data. Providing the trustworthiness of collected information must be done on every layers of IoT system.

Trust Management Mechanism (TMM) comprise a number components such as secure routing, authorization and authentication, etc. This study focused on secure routing (Fig. 2). There is need to optimize all characters of paths simultaneously because each of them is independent of the other. Thus, the following mathematical description of characters is proposed for optimization:

$$\text{Optimize Security}(S_1, S_2, ..., S_n)$$
$$\text{Privacy}(P_1, P_2, ..., P_n)$$
$$\text{Cost}(C_1, C_2, ..., C_n)$$

$$\text{Security} \equiv f(\text{considentiality, integrity, availability})$$
$$\text{Privacy} \equiv g(\text{protection})$$
$$\text{Cost} \equiv h(\text{bandwidth, price, traffic})$$

$$\text{S.T: } i \in \{1, ..., n\}: S_i \geq PS, P_i \geq PP$$
$$\sum_{i=1}^{n} C_i \leq PC \quad (10)$$

where, S_i, P_i, C_i are 'security', 'privacy' and 'cost' for the each path, respectively. 'Security' for each path must be greater than or equal to predefined degree of 'security' (PS) and also 'privacy' for each path must be greater than or equal to predefined degree of 'Privacy' (PP). Total 'cost' of selected paths must be less than or equal to predefined degree of 'cost'. 'Security' means a function of 'confidentiality', 'integrity' and 'availability'. 'Security' is defined from administrator viewpoint and 'privacy' is in contrast with it from the user viewpoint. In other words, the administrator uses 'security' to measure different paths but the user uses 'privacy' to determine safe paths. 'Cost' is defined with IoT provider organization and determines the suitable path from its viewpoint. All variables (confidentiality, integrity, availability, protection, bandwidth, price and traffic) are specific for each path and are independent of each other.

MOLA was used to solve in this study (Rahman and Choo, 2015). Actually, learning parameters have influence on final result, therefore, different ways to tune learning parameters were examined. MOLA permits the location of a path for communication with optimum values of its variables.

RESULTS AND DISCUSSION

The characters of network are represented for 'security', for 'privacy' and for 'cost'. As mentioned already, 'security', 'privacy' and 'cost' are functions from number variables. Different methods such as aggregation, fuzzy and so on can be used to define those functions but the tables show just the final values of the functions.

Values for 'security'

0.5470	0.7242	0.5666	0.9440	0.7888	0.3225	0.0728	0.9223	0.5383	0.9519
0.3249	0.8325	0.7040	0.5684	0.3632	0.4684	0.2064	0.4869	0.8783	0.0843
0.7681	0.4590	0.3539	0.9525	0.3613	0.7009	0.9015	0.2978	0.8177	0.0838
0.3178	0.7493	0.9031	0.7294	0.4458	0.8597	0.5312	0.5415	0.6849	0.3262
0.1024	0.1525	0.4544	0.7902	0.7086	0.3051	0.2343	0.6153	0.2845	0.8290
0.0522	0.3202	0.9393	0.2211	0.8195	0.8951	0.9904	0.4900	0.6602	0.7120
0.2138	0.1037	0.2413	0.4132	0.8610	0.7795	0.3848	0.1138	0.8478	0.9258
0.8094	0.2684	0.2273	0.2584	0.8237	0.7081	0.2038	0.6506	0.3397	0.9508
0.6065	0.8587	0.2856	0.5046	0.3833	0.0558	0.4217	0.7502	0.0962	0.7503
0.4090	0.6653	0.2992	0.8838	0.9506	0.0846	0.0731	0.3619	0.3479	0.2060

Values for 'privacy'

0.4030	0.6137	0.8113	0.8715	0.4730	0.9761	0.7512	0.3270	0.4633	0.0763
0.3989	0.9954	0.9323	0.3808	0.4076	0.5034	0.3386	0.2622	0.0610	0.5632
0.2331	0.8610	0.3472	0.2982	0.7416	0.0062	0.3183	0.1250	0.9812	0.3377
0.9844	0.8419	0.1051	0.7175	0.5088	0.6777	0.9559	0.2817	0.2083	0.8808
0.9591	0.1556	0.6689	0.7127	0.9581	0.7898	0.4647	0.1226	0.7357	0.9351
0.5712	0.4929	0.4823	0.0959	0.7715	0.6843	0.0337	0.5835	0.0523	0.4879
0.6457	0.3775	0.6229	0.2178	0.2839	0.9548	0.1626	0.1588	0.5828	0.5751
0.6088	0.2581	0.0486	0.1979	0.8106	0.8594	0.9933	0.2152	0.1979	0.3946
0.7146	0.9205	0.7968	0.6107	0.7287	0.1382	0.4113	0.9810	0.3846	0.9766
0.9950	0.9643	0.5311	0.4044	0.4606	0.5822	0.5806	0.7248	0.9617	0.7682

Values for 'cost'

0.1070	0.7830	0.5768	0.5076	0.8288	0.2782	0.8312	0.8041	0.8208	0.7087
0.2681	0.6498	0.6877	0.6346	0.3687	0.9105	0.5741	0.5796	0.4409	0.5393
0.5874	0.6608	0.2537	0.1584	0.7059	0.3743	0.5971	0.3884	0.8620	0.2361
0.5483	0.1669	0.7451	0.1334	0.5305	0.8058	0.0667	0.4809	0.6082	0.1334

0.1529	0.0896	0.8313	0.4726	0.5058	0.2364	0.6194	0.1238	0.4113	0.3991
0.7477	0.2217	0.5400	0.0602	0.1957	0.6568	0.4243	0.0833	0.5568	0.6176
0.3806	0.2629	0.5229	0.8586	0.6154	0.9196	0.7968	0.3558	0.5862	0.0100
0.4799	0.4810	0.1692	0.6057	0.8022	0.7811	0.0936	0.2439	0.5068	0.5845
0.4015	0.7508	0.1428	0.7038	0.8873	0.8631	0.9591	0.2335	0.5003	0.4929
0.2610	0.6712	0.0015	0.3012	0.2876	0.1531	0.2870	0.8583	0.9536	0.6155

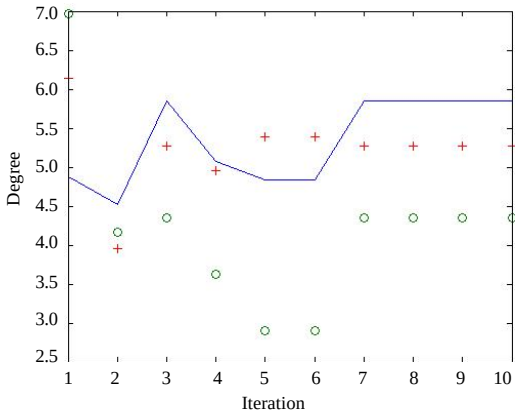

Fig. 3: Results of the first approach (a = b)

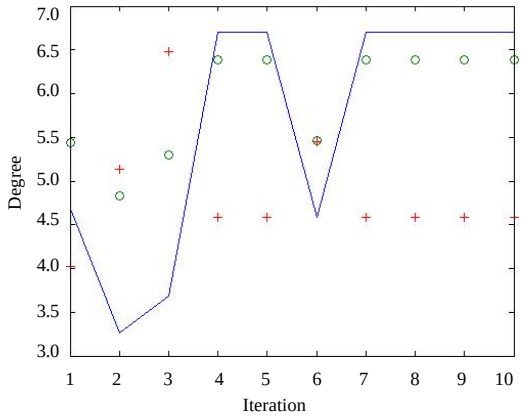

Fig. 4: Results for the second approach (b«a)

There exist three approaches to learning automata according to Nehme *et al*. (2008). The results of different approaches are presented in Fig. 3-5. In all figures, line '-' represents 'security', line 'o' represents 'privacy' and line '+' represents 'cost'.

Figure 3-5 present results of proposed approach. The horizontal line in Fig. 3-5 indicates the iterations of algorithm. The vertical axis indicates the value of each parameter that different learning methods generate.

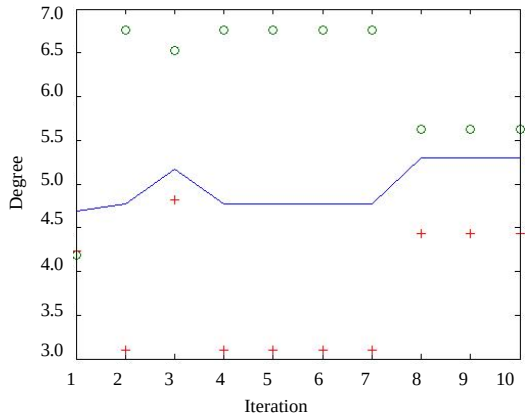

Fig. 5: Results for the third approach (b = 0)

The protracted line is for 'security'. 'o' line presents values of 'privacy'. the '*' line presents values of 'cost'.

As we can see in Fig. 3-5, the first approach (a = b) has the best performance but it reach to stable state latter than the second approach (b«a) and the third approach (b = 0). Actually, combination of these approaches may cause better results but it is subject for another paper.

CONCLUSION

In this study, secure routing of security mechanism for IoT systems was the main concerns. The proposed approach was based on optimization, so, the first step involved the definition of secure routing as an optimization problem. 'Security', 'privacy' and 'cost' were considered as influenced parameters in optimization model. 'Security', 'privacy' and 'cost' were defined as independent values but we can consider them as functions in future works.

Multi-Objective Learning Automata (MOLA) is used to solve proposed optimization problem. There are three approaches to train LA and their results have been

presented in this study. Each approach produces different results which have different values in rate of convergence and optimum value viewpoints.

RECOMMENDATION

For future studies, combined algorithm is proposed which has advantages over all three algorithms.

REFERENCES

Abomhara, M. and G.M. Koien, 2014. Security and privacy in the internet of things: Current status and open issues. Proceedings of the 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), May 11-14, 2014, IEEE, Aalborg, Denmark, ISBN:978-1-4799-4630-3, pp: 1-8.

Alcaide, A., E. Palomar, J. Montero-Castillo and A. Ribagorda, 2013. Anonymous authentication for privacy-preserving IoT target-driven applications. Comput. Secur., 37: 111-123.

Bose, T., S. Bandyopadhyay, A. Ukil, A. Bhattacharyya and A. Pal, 2015. Why not keep your personal data secure yet private in IoT?: Our lightweight approach. Proceedings of the 2015 IEEE 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP'15), April 7-9, 2015, IEEE, Singapore, ISBN:978-1-4799-8054-3, pp: 1-6.

Curilem, S.G., A.R. Barbosa and F.M. De Azevedo, 2007. Intelligent tutoring systems: Formalization as automata and interface design using neural networks. Comput. Educ., 49: 545-561.

Durisic, M.P., Z. Tafa, G. Dimic and V. Milutinovic, 2012. A survey of military applications of wireless sensor networks. Proceedings of the 2012 Mediterranean Conference on Embedded Computing (MECO'12), June 19-21, 2012, IEEE, Bar, Montenegro, ISBN:978-1-4673-2366-6, pp: 196-199.

Furtado, H. and R. Trobec, 2011. Applications of wireless sensors in medicine. Proceedings of the 34th International Conference on Convention MIPRO 2011, May 23-27, 2011, IEEE, Opatija, Croatia, ISBN:978-1-4577-0996-8, pp: 257-261.

Ge, H., Y. Wang, S. Li, C.L.P. Chen and Y. Guo, 2016. A cooperative framework of learning automata and its application in tutorial-like system. Neurocomput., 188: 311-318.

Hussain, M.A. and K.K. Sup, 2009. WSN research activities for military application. Proceedings of the 11th International Conference on Advanced Communication Technology (ICACT'09) Vol. 1, February 15-18, 2009, IEEE, Phoenix Park, South Korea, ISBN:978-89-5519-138-7, pp: 271-274.

Krishna, P.V., S. Misra, V. Saritha, H. Agarwal and N. Chilamkurti, 2013. Learning automata-based virtual backoff algorithm for efficient medium access in vehicular ad hoc networks. J. Syst. Archit., 59: 968-975.

Kumar, N., R. Iqbal, S. Misra and J.J. Rodrigues, 2015. An intelligent approach for building a secure decentralized public key infrastructure in VANET. J. Comput. Syst. Sci., 81: 1042-1058.

Li, L., 2012. Study on security architecture in the internet of things. Proceedings of the 2012 International Conference on Measurement, Information and Control (MIC'12) Vol. 1, May 18-20, 2012, IEEE, Harbin, China, ISBN:978-1-4577-1601-0, pp: 374-377.

Nazareth, D.L. and J. Choi, 2015. A system dynamics model for information security management. Inf. Manage., 52: 123-134.

Nehme, R.V., E.A. Rundensteiner and E. Bertino, 2008. A security punctuation framework for enforcing access control on streaming data. Proceedings of the 2008 IEEE 24th International Conference on Data Engineering (ICDE'08), April 7-12 2008, IEEE, Cancun, Mexico, ISBN:978-1-4244-1836-7, pp: 406-415.

Ojamaa, A., E. Tyugu and J. Kivimaa, 2008. Pareto-optimal situaton analysis for selection of security measures. Proceedings of the 2008 IEEE International Conference on Military Communications (MILCOM'08), November 16-19, 2008, IEEE, San Diego, California, USA., ISBN:978-1-4244-2676-8, pp: 1-7.

Palattella, M.R., N. Accettura, L.A. Grieco, G. Boggia and M. Dohler *et al*., 2013. On optimal scheduling in duty-cycled industrial IoT applications using IEEE802.15.4e TSCH. IEEE. Sens. J., 13: 3655-3666.

Pohls, H.C., V. Angelakis, S. Suppan, K. Fischer and G. Oikonomou *et al*., 2014. RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects. Proceedings of the 2014 IEEE Workshops on Wireless Communications and Networking Conference (WCNCW'14), April 6-9, 2014, IEEE, Istanbul, Turkey, ISBN:978-1-4799-3086-9, pp: 122-127.

Potter, C.H., G.P. Hancke and B.J. Silva, 2013. Machine-to-machine: Possible applications in industrial networks. Proceedings of the 2013 IEEE International Conference on Industrial Technology (ICIT'13), February 25-28, 2013, IEEE, Cape Town, South Africa, ISBN:978-1-4673-4567-5, pp: 1321-1326.

Rahman, N.H.A. and K.K.R. Choo, 2015. A survey of information security incident handling in the cloud. Comput. Secur., 49: 45-69.

Saha, S. and M. Matsumoto, 2007. A framework for disaster management system and WSN protocol for rescue operation. Proceedings of the 2007 IEEE Region 10 Conference on TENCON, October 30-November 2, 2007, IEEE, Taipei, Taiwan, ISBN:978-1-4244-1271-6, pp: 1-4.

Schurgot, M.R., D.A. Shinberg and L.G. Greenwald, 2015. Experiments with security and privacy in IoT networks. Proceedings of the 2015 IEEE 16th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'15), June 14-17, 2015, IEEE, Boston, Massachusetts, ISBN:978-1-4799-8461-9, pp: 1-6.

Torkestani, J.A. and M.R. Meybodi, 2010. An intelligent backbone formation algorithm for wireless ad hoc networks based on distributed learning automata. Comput. Networks, 54: 826-843.

Unger, S. and D. Timmermann, 2015. DPWSec: Devices profile for web services security. Proceedings of the 2015 IEEE 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP'15), April 7-9, 2015, IEEE, Singapore, ISBN:978-1-4799-8055-0, pp: 1-6.

Xu, T., J.B. Wendt and M. Potkonjak, 2014. Security of IoT systems: Design challenges and opportunities. Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, November 03-06, 2014, IEEE, San Jose, California, USA., ISBN:978-1-4799-6277-8, pp: 417-423.