SecureIoT: Hop-Count Based Service-Oriented Efficient Security Solution for IoT

Pushpendu Kar, *Member*, *IEEE*
Department of ICT and Natural Sciences,
Norwegian University of
Science and Technology, Norway
pushpendu.kar@ntnu.no

Sudip Misra, *Senior Member*, *IEEE*
Department of Computer Sc. and Engg.
Indian Institute of Technology
Kharagpur, India
smisra@sit.iitkgp.ernet.in

Ankush Kumar Mandal
Department of Computer Sc. and Engg.
National Institute of Technology Durgapur
India, 713209
mandalankush96@gmail.com

Hao Wang, *Member*, *IEEE*
Department of ICT and Natural Sciences,
Norwegian University of
Science and Technology, Norway
hawa@ntnu.no

ABSTRACT

Internet of Things (IoT) is a network of physical devices which are accessible through the Internet. All the devices are assigned with an IP address and are competent enough to collect data and provide some services. The installed technology and software used in all these smart items help them to interact with the end-user(s). Thus the IoT network becomes more vulnerable to attacks by external entities. Consequently, it is required to check the leakage of any information during message transmission in the network. Message injection, relay attacks, and side channel attacks by a malicious node can result in privacy loss and security hacks. Service-Oriented Architecture help vendors provide services to the consumer over a network following some protocols. In this paper we have implemented a security scheme that can be suitable for Service Oriented Architecture (SOA) based IoT network. The proposed scheme allows to transfer data in a network only if the public key (encrypted hop-count) received by the packet matches with the public key(decrypted hop-count) between the source and destination node stored in the routing table. Otherwise, the data are considered to be malicious and discarded from the network. A non-cooperative Stackelberg game based mathematical model is presented, which considers defenders as leaders and attackers as followers. We have simulated our proposed scheme and have compared it with the existing security and authentication scheme, UAKMP, in identical conditions. From the analysis of the results we evaluate that, SecureIoT has improved performance with reduced communication overheads.

KEYWORDS

IoT, Stackelberg Game, Hop-count, SOA, Malicious nodes, Privacy, Security

1 INTRODUCTION

IoT is the network of different heterogeneous devices (components) which connect via the Internet and communicate with one another. It is actually the network of physical devices embedded with software, sensors, actuators, which help in communication in IoT. IoT devices collect useful data, pass it through the gateway, send the data to cloud storage, where data are processed and finally, the results of analysis are sent to the devices as information to the users. As the devices are connected to the network, security and privacy become very important issues for theses devices.

Most of the previous research works in this domain (eg. [7]) use crypto-analysis, encryption-decryption and private-public key methodology. The authors in [7] have resolved security issues at different layers – Perception, network, application – of the IoT network. They have assessed different types (remote and local) and mode of attacks. However, when an adversary attacks a network and channelizes malicious data inside it, the entire network becomes corrupted and the whole data become compromised.

So, we need an efficient scheme to protect the network from the attacks by external entities. In SOA, services play an important role as they communicate among themselves through normal data communication or co-ordinate for a joint-service. In web services, the entire transmission is dependent on the connection between two services, which involves request and the corresponding response. Here we want to integrate the IoT security problem with a service architecture, which would increase its usability in other networks also.

In many previous research works, game theory was used as an important tool to represent network security model. In earlier references, many frameworks have proposed three-way handshake based security schemes for service-oriented architectures. In the proposed scheme, we have introduced two-way handshake based security by the use of routing table. The main motivation of using Stackelberg game theoretical model in our paper is to model the attacker-defender scenario. Here, the defender takes its own strategy, while the attacker decides a strategy following the defender. Thereafter, we find Nash Equilibrium of the proposed game, where the payoffs for both of the parties are maximized after both of them have chosen their optimum strategies.

In many existing works, different security issues of IoT network were addressed, but they seldom proposed any security scheme which can limit the attacks of an adversary. In this work, we plan to target that security gap of IoT by proposing the scheme, SecureIoT, and then integrating it with SOA to make the network more robust. In this paper, we address the issue of an adversary attacking and gaining control of one of the nodes in the network. We present the idea of providing a secure centralized network with

the help of hop-count–our IoT security parameter for successful data communication–and the specialized routing table.

The attacker node or adversary are supposed to attack the important network components in an IoT network by code injection, DoS attacks, spoofing attacks, sinkhole or wormhole attacks. After getting control over the regular network nodes, the attacker node can intercept any message (because of the source node not knowing that the node has been hijacked), but cannot open or read it, because it does not have the decryption key. As soon as the attacker attacks a node, all the other network nodes become alert and reject any message that the malicious node sends as it does not know the exact hop length between the nodes. An attacker does not get to know the routing table, as it is created only by every network nodes in the IoT network. Therefore, the malicious nodes cannot know the hop-count to any of the network nodes. Consequently, they also have no idea about the creation of a public key to encrypt the data message for a secured communication.

We have attempted to account for the shortfalls of IoT security schemes. The proposed scheme is a new technique of network security in the service-oriented architecture. This scheme improves the data rate in communication, as the nodes already know their hop-counts, which are used for message encryption as public key without exchanging public key between source and destination. In this paper, we have proposed an enhanced security solution for an IoT network in the backdrop of SOA. The overall contributions of this work are summarised as follows:

(1) We proposed a scheme, named SecureIoT, for the security of a service oriented network.
(2) We have mathematically modelled the scheme.
(3) We have evaluated simulation-based performance of the proposed scheme.
(4) We have performed simulation based comparison of the proposed scheme with the state-of-the-art.

2 LITERATURE REVIEW

Several works [4] in the existing literature address issues concerning the safety of networks. Smart devices connected with Internet can integrate to form an IoT network, but the security solutions need to be extended to provide security for the IoT applications. In this section, we discuss the different security implementations in different layers of the IoT network. Perception layer security deals with the acquisition and collection of data through various collecting and controlling modules such as temperature sensors and pressure sensors. In this layer, the adversary's main motive [15] [3] is to forge stacked up raw data and destroy the perception devices. Using false data injection, the attacker copies malignant data inside the vicious nodes. Thereafter the node collects garbage data, which leads the network to flow erroneous data. Data filtering techniques should be designed and implemented to stop this type of attacks [8] [9].

The devices [1, 16] connected to the Internet allow them to communicate, interact, and connect with one another. The devices also co-operate with one another, which also increases service demand in the service oriented architecture. As we know, the embedded systems industry is drifting towards the use of service-oriented architecture for IoT [10]. The main problem with these systems is that the devices always have to be connected with one another. The interaction between the user and connecting devices is important for security reasons. The Internet is connected to the physical world through the exchange of semantic knowledge. External entities get access to the gateways and other resources meant for the services in a service-oriented architecture [6], which calls for the privacy and security of personal data.

Webb [13] explained the Stackelberg duopoly model, where both the firms have to compete against each other for the same set of customers with their products. Here, the leader firm makes its decision and all the followers have to prepare strategies based on the leader's strategy. Han et al. [5] explained that, in some cases, players play games without knowing the opponents preference (payoffs), which leads to Bayesian games. This framework is often used to analyze wireless transmission networks. These security games [2] between attackers (selects the target) and defender (allocates resources) and performs as follows.

- The defender considers the best response of the attacker (which target will be attacked).
- The defender selects the resources accordingly.
- The target optimizes its best attack keeping in mind the defender's best response to its attack.

Wilczynski et al. [14], mentions different models of Stackelberg game theory, which have been implemented earlier to map the attacker-defender scenarios in different security implementations. Wazid et al. [12] provided a security scheme (UAKMP) for key management in IoT networks. In this scheme, a gateway node connects users and service providers (sensory nodes), which provides security and authentication by using public key and smart cards.

3 SYSTEM MODEL

In the proposed security scheme, we assumed that every node knows its respective hop-count from its neighbour nodes. When a service is requested by a user, the request reaches the middleware, which checks the request and verifies if that particular request is a service provided by the provider. This layer acts as a service broker and it also contains the SLA (Service Layer Agreement) [11]. The SLA document consists of two things namely 1) price for using the network and 2) level of security provided. This document has a middle ground agreement in which the provider and the consumer agree. If the request satisfies the agreement, it passes the request to the provider. The provider executes the service and passes the results to the user through the IoT devices. In this paper, we have tried to make use of hop-count as our parameter for IoT security. After the change of network topology every node updates its routing table and checks the hop-count to the next hop, where the data needs to be sent.

This model provides data security from any kind of data tampering or manhandling. Each and every node and knows its hop distance from its adjacent nodes. When an adversary attacks by implementing a malicious node in the network, the new node in the network does not know its hop-count from its neighbours. So it does not be able to send any data into the network, as nodes only accept data if the node is the actual recipient who knows the actual hop-count from the source. Otherwise, the data is dropped from the

network. In this manner the proposed scheme prevents erroneous data flow in the network.

The proposed scheme works in any condition whether the source node is malicious or not. When the source node is malicious, it does not know where to send the data. As the malicious node has no knowledge of the hop-count for the next neighbour node, it cannot transfer the data in the network, thereby dropping the data. In this manner, the entire security protocol does not depend silelly on the source node and works seamlessly even when the source node is malicious.

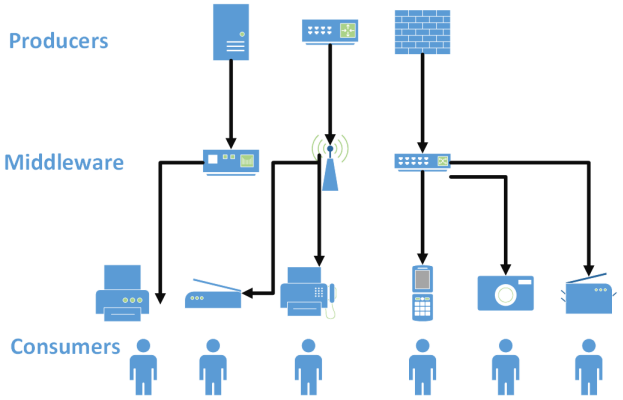

Figure 1: SOA in IoT

In Figure 1, we have integrated the idea of SOA in an IoT network and highlighted its various components. The producer nodes generate the various web services and the consumers are the smart devices possessed by users. e.g. personal computer, mobiles, watches, smart homes. The middle layer or the middleware is the interface between the producer and the consumer where both the parties submit their requirements for interaction between them. The consumers at first contact the middleware and ask them to check the various kinds of services provided by the producers. The middleware then checks their quantity, cost, and quality requirements and then matches with the best possible service provided. The two sets of documents provided by both the parties are also known as the Service Layer Agreement (SLA). It mainly functions as the broker between the service producers and the service consumers.

4 PROPOSED SOLUTION

The security function $A(s)$ has the maximum value A_0 when the network is fully secured and it reduces to 0 when the network is sabotaged. The network cost of any device in a network is directly proportional to the security factor provided by that device. Let s_i be any strategy chosen by a network node n_i. The network cost is computed as follows

$$C(s) = C_i s_i \tag{1}$$

for the i^{th} node in the network. Say C_1 be the cost for data transmission (constant of proportionality) in the network. The cost for defender is,

$$C(s_1) = C_1 s_1 \tag{2}$$

We assume thet the attacker attacks when the exact encrypted hop-count from the routing table is known. The cost of network transmission for the attacker is,

$$C(s_2) = C_2 s_2 \tag{3}$$

The total security of the network is:

$$A = A_0(1 - s) \tag{4}$$

where s is the net security in the IoT network and

$$s = s_1 - s_2 \tag{5}$$

Let the profit function be $A(s_1, s_2)$, which is the total security of the IoT network without the network cost for a particular node. The profit function for the nodes in the network:

$$A(s_1, s_2) = A_0(1 - s) - Cs_i \tag{6}$$

As attackers already know the choice of the defenders, so they make the best possible response $s_2(s_1)$ for the certain choice of defenders. To attain Nash Equilibrium, we need the maximum payoff of the defenders. The attacker's profit function is given by $P(q_2, q_1)$ and the best response to any choice q_1 is found by partially differentiating the profit function with respect to s_2.

$$\frac{\partial A(s_1, s_2)}{\partial s_2} = 0$$

which gives

$$\begin{aligned} 0 &= \frac{\partial((A_0(1 - s) - C)s_2}{\partial s_2} \\ &= A_0(1 - s_1 + 2s_2) - C \\ s_2(s_1) &= \frac{\frac{C}{A_0} - 1 + s_1}{2} \end{aligned} \tag{7}$$

So, the defender maximizes its security payoff function by choosing the following strategy:

$$\begin{aligned} \frac{\partial A(s_1, s_2)}{\partial s_1} &= 0 \\ 0 &= \frac{\partial(\frac{s_1 A_0}{2} - \frac{s_1^2 A_0}{2} - \frac{s_1 C}{2})}{\partial s_1} \\ s_1^* &= \frac{1}{2A_0}(A_0 - C) \\ s_1^* &= \frac{1}{2}(1 - \frac{C}{A_0}) \end{aligned} \tag{8}$$

4.1 Nash Equilibrium

The proposed security scheme, SecureIoT, reaches an equilibrium point, where both the parties (attackers and defenders) have the maximum payoff. That point in a game theoretic model is referred to as Nash Equilibrium point. The respective most optimal strategies for both attackers are:-

$$\begin{aligned} s_1^* &= \frac{1}{2}(1 - \frac{C}{A_0}) \\ s_2^* &= \frac{1}{4}(\frac{C}{A_0} - 1) \end{aligned} \tag{9}$$

The solutions above constitute of the mixed strategy sub-game perfect Nash equilibrium for the security Stackelberg game between the attacker and the defender. The attacker chooses an attacking strategy after knowing the defender's strategy, while the defender chooses any strategy of its choice.

4.2 The proposed algorithm

In SecureIoT, the network nodes update their routing table when there is a change in the topology by broadcasting 'Hello' messages in the network shown in Algorithm 1. The creation of a routing table is the first phase of the proposed scheme. Every node, on receiving the message, first checks in the routing table the hop-count value and then transmits the data. Any external malicious node does not have information regarding the routing table and the hop-count value to reach the next neighbour node. If a node tries to communicate with any other node with an arbitrary hop-count, it fails to do so, as the received hop-count from the packet does not match with hop-count from the source and the destination stored in the routing table.

Algorithm 1 SecureIoT

Inputs:
$NODE_{id}$: unique ID of NODES
$rou\_table[][]$: routing table
h_{ij} : Hop count between two nodes i and j
Output:
prn: Indicates received or not received; if value = 0 pkt is not received else received

Begin
for i=1 to N **do**
  for j=1 to N **do**
    $rou\_table[i][j] \leftarrow h_{ij}$
  end for
end for
if $packet \neq 0$ **then**
  $p_h \leftarrow$ hop count of the received packet
  $s_{id} \leftarrow$ source id of the received packet
  $d_{id} \leftarrow$ destination id of the received packet
end if
if $p_h == rou\_table[s_{id}][d_{id}]$ **then**
  $prn \leftarrow 1$
else
  $prn \leftarrow 0$
end if
return prn
End

Based on the number of intermediate nodes, a message takes time to traverse from the source to the destination. A message is successfully transmitted from a node to another node, as long as both the nodes know their hop-count from each other. However, if any malicious node attacks without knowing the hop-count to the destination node, then that data does not reach the destination node.

5 SIMULATION RESULTS

5.1 Simulation Configuration

In this section, we evaluate the performance of the proposed security scheme, SecureIoT, for understanding its capability. The proposed scheme has simulated using the MATLAB simulator. We deployed 50-300 nodes over a contour of 500×500m, randomly. We have simulated our proposed scheme n^2 times, where n is number of nodes in the network. We also have compared the proposed scheme, SecureIoT, with UAKMP, which is a three-steps user authentication scheme for hierarchical IoT networks. It also provides several security features such as offline node sensing, freely password and bio-metric update facility. Additionally, the scheme is comparable in terms of computation and communication costs. So, we compared the proposed scheme with this scheme. Table 1 presents the simulation parameters and their corresponding values.

Table 1: SIMULATION PARAMETERS

Parameter	Value
Number of nodes	150-300
Increase in number of nodes for each simulations	50
Number of node levels	4
Simulation area	$500m \times 500m$
Range of maximum edge lengths in the network	72-82

We have done the simulation of our proposed scheme, SecureIoT, using MATLAB simulator. We have evaluated the performance of the proposed scheme using the following parameters:

(1) *Attacking Probability*: The probability of attacking by the malicious nodes to the network nodes.
(2) *Message Overhead*: The number of messages transmitted during the execution of the proposed scheme.
(3) *Computation time*: The time required for one unit of execution of the proposed scheme.

5.2 Results and Discussion

The attacking probability of attacker nodes is calculated as the ratio of the number of times the attacker successfully attacks the network nodes to the total number of attacking attempts. In the plot shown in Figure 2, we can see that, with the increase in value of hop-count the attacking probability also increases. The possible reason behind this is that, the increase in the value of hop-count increases the chances of matching the hop-count in the routing table. We also see that the increase in number of nodes increases the attacking probability, because the chances of matching the hop-count with any of the nodes in the network also increases.

Figure 3 shows that the message overhead increases with the increase in the number of nodes in the network. The possible reason is that, the increase in the number of nodes increases the number of message exchanged in the network. Hence, the total number of messages exchanged (message overhead) in the proposed scheme also increases with the increase in the number of nodes in the network,

The plot for computation time in Figure 4 shows that the network for more number of nodes require more computation time to execute the proposed scheme. The possible reason is that, with the increase in number of nodes, the size of routing table as well as the number of routing table also increases. Time taken for creation of the routing table consumes major part in computation time of the proposed scheme. Therefore, the computation of the proposed

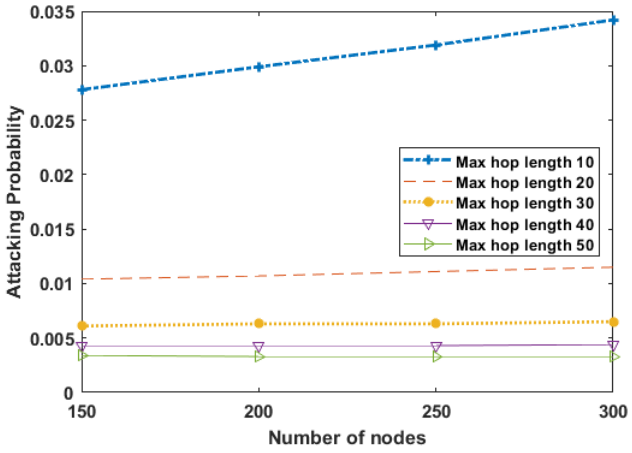

Figure 2: Attacking Probability

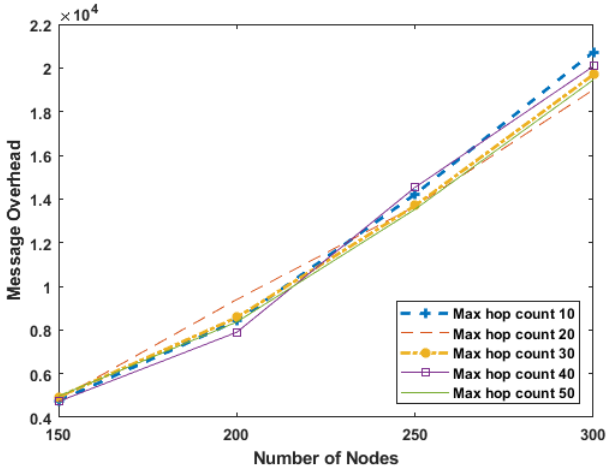

Figure 3: Message Overhead

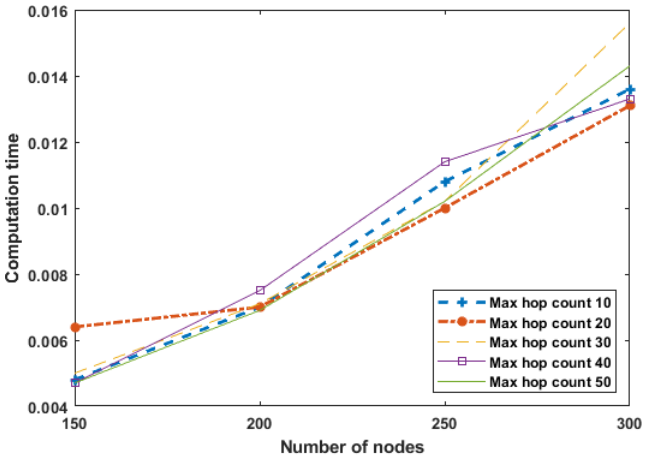

Figure 4: Computation time

scheme increases with the increase in the number of nodes in the network.

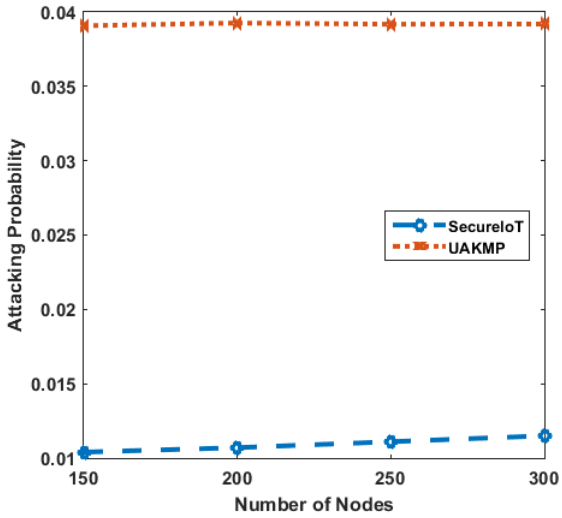

Figure 5: Comparison of the scheme

Comparison of the proposed scheme with the benchmark IoT security scheme, UAKMP, is shown in Figure 5. The plot shows that the attacking probability for UAKMP is much higher than that of the proposed scheme because UAKMP required exchange of more number of messages through gateway, which makes the scheme more vulnerable for attacking.

6 CONCLUSIONS

In this work, we proposed an IoT security scheme, SecureIoT, for a service oriented IoT network. In this scheme, the hop-count between the sender and the receiver nodes used as public key to encrypt messages exchanged between the corresponding pair of nodes. A receiver node receives a message, if the hop-count extracted from the message matches with the hop-count value of the corresponding pair of nodes stored in the routing table. As a malicious node cannot know the hop-count to a attacking node, the node does not become succeeded in injecting malicious data in the network nodes. The proposed scheme eliminates the first step (exchange of public key) from the general IoT security scheme and makes it faster than the existing IoT security schemes. Simulation results show that the proposed scheme outperforms the chosen benchmark security scheme in terms of attacking probability. The limitation of SecureIoT is that it fails to secure the insignificant networking devices, which only forward data packets but do not store routing-table.

In the future, we plan to implement the proposed security scheme on a real test-bed and try to improve its security domain for all the networking devices in an IoT network.

REFERENCES

[1] Ray Chen, Jia Guo, and Fenye Bao. Trust management for service composition in soa-based iot systems. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, pages 3444–3449, Istanbul, Turkey, April 2014.

[2] Julio B Clempner and Alexander S Poznyak. Stackelberg security games: Computing the shortest-path equilibrium. *Expert Systems With Applications*, 42(8):3967–3979, 2015.

[3] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3):1294–1312, 2015.

[4] KrishnaKanth Gupta and Sapna Shukla. Internet of things: Security challenges for next generation networks. In *Proceedings of the IEEE International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, pages 315–318, Noida, India, August 2016.

[5] Zhu Han, Dusit Niyato, Walid Saad, Tamer Başar, and Are Hjørungnes. *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge university press, 2012.

[6] Valérie Issarny, Georgios Bouloukakis, Nikolaos Georgantas, and Benjamin Billet. Revisiting service-oriented architecture for the iot: a middleware perspective. In *Proceedings of the International Conference on Service-Oriented Computing*, pages 3–17, Macau, China, 2016.

[7] Shivaji Kulkarni, Shrihari Durg, and Nalini Iyer. Internet of things (iot) security. In *Proceedings of the* 3^{rd} *IEEE International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 821–824, Banff, Alberta, Canada, 2016.

[8] Jie Lin, Wei Yu, and Xinyu Yang. Towards multistep electricity prices in smart grid electricity markets. *IEEE Transactions on Parallel and Distributed Systems*, 27(1):286–302, 2016.

[9] Jie Lin, Wei Yu, Xinyu Yang, Guobin Xu, and Wei Zhao. On false data injection attacks against distributed energy routing in smart grid. In *Proceedings of the IEEE/ACM Third International Conference on Cyber-Physical Systems(ICCPS)*, pages 183–192, Beijing, China, April 2012.

[10] Weigong Lv, Fanchao Meng, Ce Zhang, Yuefei Lv, Ning Cao, and Jianan Jiang. Research on unified architecture of iot system. In *Proceedings of the IEEE International Conference on Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC)*, volume 2, pages 345–352, Guangzhou, Guangdong, China, July 2017.

[11] Benay Kumar Ray, Sunirmal Khatua, and Sarbani Roy. Negotiation based service brokering using game theory. In *Proceedings of the IEEE Applications and Innovations in Mobile Computing (AIMoC)*, pages 1–8, Kolkata, India, February 2014.

[12] Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, and Minho Jo. Design of secure user authenticated key management protocol for generic iot networks. *IEEE Internet of Things Journal*, 5(1):269–282, 2018.

[13] James N Webb. *Game theory: decisions, interaction and Evolution*. Springer Science & Business Media, 2007.

[14] Andrzej Wilczyński, Agnieszka Jakóbik, and Joanna Kołodziej. Stackelberg security games: Models, applications and computational aspects. *Journal of Telecommunications and Information Technology*, 2016.

[15] Xinyu Yang, Jie Lin, Wei Yu, Paul-Marie Moulema, Xinwen Fu, and Wei Zhao. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. *IEEE Transactions on Computers*, 64(1):4–18, 2015.

[16] Yang Zhang, Li Duan, and Jun Liang Chen. Event-driven soa for iot services. In *Proceedings of the IEEE International Conference on Services Computing (SCC)*, pages 629–636, Anchorage, Alaska, USA, February 2014.