International Journal of Emerging Technology and Advanced Engineering  

Study on Smart Car-Parking System Using IoT

Vrushali U. Uttarwar¹, Jayant K. Shimpi²
¹²Assistant Prof. Dept. of Computer Engg., D. Y. Patil College of Engg., Akurdi, Pune., India
¹emailvrushali@gmail.com  
²jayant.shimpi2018@gmail.com

Abstract—Internet of Things (IOT) plays a vital role in connecting the surrounding environmental things to the network and made easy to access those un-internet things from any remote location. It’s inevitable for the people to update with the growing technology. And generally people are facing problems on parking vehicles in parking slots in a city. In this study we design a Smart Parking System (SPS) which enables the user to find the nearest parking area and gives availability of parking slots in that respective parking area. And it mainly focus on reducing the time in finding the parking lots and also it avoids the unnecessary travelling through filled parking lots in a parking area. Thus it reduces the fuel consumption which in turn reduces carbon footprints in an atmosphere. This paper introduces a novel algorithm that increases the efficiency of the current cloud-based smart-parking system and develops a network architecture based on the Internet-of-Things technology. This paper proposed a system that helps users automatically find a free parking space at the least cost based on new performance metrics to calculate the user parking cost by considering the distance and the total number of free places in each car park. This cost will be used to offer a solution of finding an available parking space upon a request by the user and a solution of suggesting a new car park if the current car park is full. The simulation results show that the algorithm helps improve the probability of successful parking and minimizes the user waiting time. We also successfully implemented the proposed system in the real world.

Keywords— Internet of Things; Smart-parking system, performance metrics.

I. INTRODUCTION

In the development of traffic management systems, an intelligent parking system was created to reduce the cost of hiring people and for optimal use of resources for car-park owners. Currently, the common method of finding a parking space is manual where the driver usually finds a space in the street through luck and experience. This process takes time and effort and may lead to the worst case of failing to find any parking space if the driver is driving in a city with high vehicle density. The alternative is to find a predefined car park with high capacity. However, this is not an optimal solution because the car park could usually be far away from the user destination. In recent years, research has used vehicle-to-vehicle and vehicle-to-infrastructure interaction with the support of various wireless network technologies such as radio frequency identification (RFID), wireless mess network and the Internet. This study aimed to provide information about nearby parking spaces for the driver and to make a reservation minutes earlier using supported devices such as smartphones or tablet PCs. Furthermore, the services use the ID of each vehicle in booking a parking space. However, the current intelligent parking system does not provide an overall optimal solution in finding an available parking space, does not solve the problem of load balancing, does not provide economic benefit, and does not plan for vehicle-refusal service. To resolve the aforementioned problems and take advantage of the significant development in technology, the Internet-of-Things technology (IoT) has created a revolution in many fields in life as well as in smart-parking system (SPS) technology. The present study proposes and develops an effective cloud-based SPS solution based on the Internet of Things. Our system constructs each car park as an IoT network, and the data that include the vehicle GPS location, distance between car parking areas and number of free slots in car park areas will be transferred to the data centre. The data centre serves as a cloud server to calculate the costs of a parking request, and these costs are frequently updated and are accessible any time by the vehicles in the network. The SPS is based on several innovative technologies and can automatically monitor and manage car parks. Furthermore, in the proposed system, each car park can function independently as a traditional car park. This research also implements a system prototype with wireless access in an open-source physical computing platform based on RFID technology using a smartphone that provides the communication and user interface for both the control system and the vehicles to verify the feasibility of the proposed system. Internet of things was first introduced in 1999 at auto-ID center and first used by Kevin Ashton. As evolving this latest burning technology, it promises to connect all our surrounding things to a network and communicating with each other with less human involvement.
Still internet of things is in beginning stage and there is no common architecture exists till today. There is lot of researches and implementations are currently being going on in all the respective areas. Thus there is no guidelines or boundaries exists to define the definition of internet of things. So depending on the context, application the internet of things has different definitions. Shortly it is defined as the things present in the physical world or in an environment are attached with sensors or with any embedded systems and made connected to network via wired or wireless connections. These connected devices are called as smart devices or smart objects. And it consists of smart machines which communicating interacting with other machines, environment, objects etc. And also it incorporates to connect any two machines, machine to human and vice-versa etc. this communication is called as M-M communication. As M-M communication is developing by the various standardization bodies such as Open Mobile Alliance (OMA), European Telecommunication Standards Institute (ETSI), Institute of Electrical and Electronic Engineers (IEEE), 3rd Generation Partnership Project (3GPP) organization have performed some activities on M-M communication [4]. It makes daily life things to equip with transceivers, sensors, actuators and microcontrollers etc. for communication. Some important benefits of internet of things includes 1) tracking behaviours; 2) enhanced situational awareness; 3) sensor driven decision analytics; 4) instantaneous control and response. Etc.

IOT technology grows in various fields of smart applications but we have not yet found boundary constraints of this technology. Some smart applications which it is implementing currently such as on smart grids, smart lighting, smart energy, smart city, smart health etc. This is broadly classified into three categories such as sensing, processing and connectivity. Whereas sensing includes sensing the speed of vehicles and humans or any objects (accelerometer), sensing of temperature, pressure etc. [9]. And these can be processing by using some processors such as network processor, hybrid processor MCU/MPU etc. And the devices are connected by using some technologies called GPS, Wi-Fi, BT/BLTE, and RFID.

II. INTERNET OF THINGS

A. Protocols and IoT stack

The IoT scale factor, the discovery limitation of stages and the requirement for arrangements that work in collaboration with existing security arrangements of the Internet, are rules that have been utilized by the working gatherings made to characterize measures, for example, the Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF). Those rules drive the working gatherings in the origination of new correspondence and security conventions that will be fundamental for future IoT applications. Such solutions are being planned in arrangement with the confines and attributes of sensor devices of low energy, low remote information rate correspondence and low handling power. Although such attributes affected past tasks that make utilization of WSNs (wireless sensor networks) isolated from the Internet, the new institutionalized arrangements are imagined to guarantee the interoperability with the current Internet standards.

It likewise empowers the gadgets to speak with outer substances in the Internet, in the perspective to IoT [4].

<table>
<thead>
<tr>
<th>Table 1: IoT Protocol Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Transport</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Medium Access Control</td>
</tr>
<tr>
<td>Physical</td>
</tr>
</tbody>
</table>

B. IEEE 802.15.4

The IEEE 802.15.4 [5] standard specifies the physical (PHY) and medium access control (MAC) layers (layers 1 and 2 of the OSI model [6], respectively) for Low Rate Wireless Personal Area Networks (LRWPANs). The MAC layer has to provide communication between two devices, which is achieved by a contention mechanism.
The IEEE 802.15.4 standard implements the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme together with a deterministic mechanism. The PHY layer transmits the frame that came from the MAC layer through the medium. In order to handle different country regulations, the IEEE 802.15.4 standard defines several working frequency bands. A compliant device must support at least one of them.

The standard has security features, providing confidentiality, authenticity and replication protection to data transmission. The several security levels enables the devices to choose the cryptography with an authentication code of varying size. When this scheme is used the authentication code validates the header (which is sent without encryption) and the payload, that can be encrypted.

C. 6LoWPAN

Specified by the RFC 4944 [7], IPv6 Over Low Power Wireless Personal Area Network (6LoWPAN) is a standard that compresses IPv6 packets in 802.15.4 frames. Its advantages includes easy connectivity with IP devices, enabling the opportunity of using the existing network infrastructure and an API widely used. 6LoWPAN has its features presented in several RFCs, such as the RFC 4944, that defines the frame format that adapts the IPv6 frame to 802.15.4 frames (that can have only up to 127 bytes). The RFC 4944 was updated by the RFC 6282 [8], enabling multicast transmissions and IPv6 extensions. The RFC 6568 [9] presents deployment scenarios. The most recent updated is contained in the RFC 6775 [10].

D. CoAP

The RFC 7252 [3], released in June of 2014, specifies the Constrained Application Protocol (CoAP), a message exchange application layer protocol for low energy, low processing power devices and constrained networks. It was designed for machine-to-machine (M2M) applications, a paradigm used in residential automation. It defines 4 message types: Confirmable, Non-confirmable, Acknowledgment and Reset. Messages of the Confirmable (CON) type must be acknowledged. On receiving a CON message, a node sends an Acknowledgment or a Reset message. The Non-confirmable (NON) messages do not require an acknowledgment, which is useful when an eventual message loss does not disrupt the application operation. Reset messages indicates that a CON or NON message was received but could not be properly processed. The CoAP protocol was designed to interact with the Hypertext Transfer Protocol (HTTP), simplifying the integration with the Internet.

It is based on compact message exchange over the UDP transport layer protocol. Messages have a header of 4 bytes followed by a token with up to 8 bytes. The CoAP protocol does not include security features, instead it uses the Datagram Transport Layer Security (DTLS) [11]. DTLS is analogous to the TLS, but for the UDP protocol. It provides integrity, authenticity, confidentiality, key management and several cryptography algorithms. However DTLS was not designed for IoT, for instance it does not support multicast, which is an advantage of the CoAP in comparison with others application layer protocols.

III. RELATED WORKS

Although the 6LoWPAN and CoAP protocols bring advancements in reducing the difference between Internet and IoT protocols, those protocols still does not achieve specifications identical to the ones of Internet, mainly for performance reasons. In this regard, it is expected that small differences will remain existing among the protocols of these technologies. Although those differences could be mitigated by translators at the network gateway, they continue to be an obstacle for implementing security between IoT and Internet devices [8]. Several security requirements must be considered in an IoT environment, in particular the communication among sensor devices. For instance, WSNs can be exposed to Internet originated attacks, such as Denial of Service (DoS). A DoS attack is a malicious attempt to consume bandwidth resource of legitimate users [11]. Such attack, when occur from several compromised nodes, are called Distributed DoS (DDoS).

A reflection attack is a DDoS attack that utilizes interne-diary hosts. The attacker floods reflectors with the source IP address set as the victim’s address. A reflector is any device that when receives a message sends a response. The difference between the request and the response sizes is explored: as the reflection factor increase, more effective is the attack, amplifying the attacker’s generated traffic [2].

There are some studies that address DoS attacks in IoT. Perakovic et al. [12] analyses the availability of services by flood attacks. Tendencies of those attacks where analyzed with data from 2013 to 2015. The analysis shows that it is increasing the number of attacks in the IP and transport layer, in comparison with attacks in the application layer. Within this context, the emerging number of IoT devices could be potential reflectors for illegitimate traffic generation. The study shows that it is increasing the rate of attacks through the Simple Service Discovery Protocol (SSDP), which is utilized in many IoT devices.
Raymond et al. [13] discuss several defense schemes against DDoS attacks in a WSN. This type of attack and its impact on the Quality of Service (QoS) of WSNs based on IP is conducted by [14]. Yu et al. [15] present a review of the main security treats in IoT, displaying a possible roadmap to deal with them. Elkhodr, Shahrestani and Cheung [16] reviewed some of the main concerns to the wide adoption of IoT, such as interoperability, management, security and privacy. Cvitic’ Vujic’ and Husnjak [17] take into account the layers of an IoT stack and discuss the treats of each one of them. Other attacks and defense strategies are discussed in [18] and [19].

IV. EXPERIMENTAL EVALUATION OF DDoS ATTACK IN IoT

This section presents an experimental evaluation of the impact of a DDoS attack in IoT context. The DDoS attack aims to explore a network stack with the CoAP protocol, performing an amplified reflection attack. The next sections present a description of the experimental scenarios, followed by the results and its analysis.

A. Simulation scenarios

The simulation scenarios are designed to evaluate the effects of a amplified reflection DDoS attack in a WSN. A common WSN network was deployed, where there is an infiltrated malicious node that sends service discovery request for all sensors with the source address as the victim, which is outside the WSN.

The simulation deploys a WSN in star topology with 5, 25, 50, 75, and 100 nodes. The devices are displayed in grid with 2 meters spacing. The coordinator is the first node of the grid, the attacker is the second and the victim is the last one. The WSN has a throughput of 96 bps for each node, since each one sends a 12 bytes packet every minute.

The simulation was conducted on the NS-3 [20] simulator, an open-source, C++, community driven, network simulator. Each sensor device was deployed with the network protocol stack shown in Figure 1. The IEEE 802.15.4 standard was utilized as the layers 1 (PHY) and 2 (MAC). The MAC operational mode is unslotted CSMA with nodes always listening for the medium when not sending a packet, this mode was chosen in order to maximize the network throughput. The layer 3 (Network) utilizes the 6LoWPAN protocol, which translates IPv6 headers to fit the 802.15.4 packet size limit of 127 bytes. The application layer deploys the CoAP protocol, which utilizes UDP as the transport layer.

B. Results and Analysis

The simulated reflection attack exploits CoAP’s resource discovery feature. The attacker sends a resource discovery request packet in multicast (for all network members). The request packet has the “/well-known/” URI path prefix, which renders a 20 byte packet size. The source IP address of the packet is changed to the victim’s one. As the network sensors receive the request packet they must send a response indicating which service they support. In this experiment the devices contain only a temperature sensor, and thus only one service, which is expected from small, low capacity devices. The response message contains 61 bytes, rendering a reflection rate of 3.05 for each device that receives the request packet.

The attacker’s data generation rate was varied to find the most optimal injection rate. Traffic was generated at 0.16 bps, 1.6 kbps, 3.2 kbps, 4.0 kbps, 8.0 kbps and 16.0kbps.

![Figure 1: Average reflection rate](image)

Fig 1: Average reflection rate

Figures 1, 2 and 3 show the average generated traffic for each node, the total amplification rate and the total generated traffic, respectively. The analysis shows that the reflection occurs with amplification, validating the concerns about using IoT for a DDoS attack. Figure 3 shows that the maximum achieved amplification rate is about 20, for scenarios with more than 5 nodes. The maximum expected amplification rate is 3.05 times the number of devices in the network, rendering 76.25 for 25 nodes, which is much higher than the maximum amplification rate achieved. This difference can be explained by the low data rate characteristic of the network, the IEEE 802.15.4 supports only 250 kbps.
In all scenarios the amplification rate decreases when the injection rate goes above 2 kbps. In the attacker’s view, this could be compensated by increasing the number of reflectors in the attack, which is a valid action, since IoT should provide millions of connected devices.

The network saturation, which is characterized by the decreasing in the amplification rate, is caused by the bandwidth saturation. The maximum injected traffic occurs in the scenario with 5 nodes, decreasing as the number of sensors increase. In order to achieve a higher amplification rate, more WSNs should be used at the same time.

However the attack’s easiness automation can be attractive, even if it may demand fine adjustment and coordination by the attacker.

V. Conclusion

This work studied the viability of using an IoT environment in an amplified reflection DDoS attack. To the best of our knowledge this was the first experimental analysis of this subject that considers the full network stack. A simulation scenario was deployed utilizing the following network protocol stack: IEEE 802.15.4, 6LoWPAN, UDP and CoAP. The simulations analysis shows that a DDoS attack can indeed explore IoT environments. Furthermore, the IoT environment itself can become a target, since its bandwidth and computing resources rapidly depletes.

Although viable, the attack requires a high number of IoT networks to be effective. Some future work is the quantification of the compromise scale. In the attacker’s point of view, it is needed to decide if the coordination and fine tune efforts in order to avoid the IoT network saturation are profitable against other attack forms. As future work we also intend to explore other possible risks arising from IoT dissemination.

REFERENCES


