MANTECH Publications

Journal of Computer, Internet and Network Security
Volume 7 Issue 2
ISSN: 2457-0176 (Online)

A Study on Cognitive Packet Networks to Ensure the Safety of Internet of Things Transactions

Gautam Kapoor[1], Manya Sharma[2]

Student[1], Assistant Professor[2]

Department of Computer Science and Engineering

Shri Rawatpura Sarkar University, Raipur

Corresponding Author's Email: - *kapoorgautam23@gmail.com[1], m_sharma43@yahoo.com[2]*

Abstract

In today's networks, the idea of Security Aware Routing has not yet gained widespread acceptance. However, the newly developed core networks that are centred on IoT present opportunities to reopen that field of research. Routing is something that we believe to be an addition to the already established network security approaches, particularly in the IoT arena. The standard set of measurements is supplemented with security and safety metrics with the implementation of security-aware routing (bandwidth, network delay, hop count, path cost, load etc.). The research demonstrates a novel strategy in which, on the basis of software-defined networks (SDN), we estimate trust connections between nodes and flows and then utilise those estimations to design SDN pathways on the basis of the Cognitive Packet Network (CPN) concept. When it comes to making judgments regarding routing, Random Neural Networks (RNN), which are backed by cognitive packets, are utilised. Within the context of the SerIoT project, the suggested solution was conceived of and is currently being put into action in order to show the viability of secure networks for the Internet of Things (IoT).

Keywords: *Se- rIoT, Internet of Things (IoT), Security, SDN, Energy, Cognitive Packet Network*

INTRODUCTION

The Internet of Things, abbreviated as IoT, refers to the portion of computer networks that is responsible for the transmission of the most confidential information. This may include data pertaining to an individual's health or location as well as information that is essential to a company's operations.

For a considerable amount of time, cybersecurity in the internet of things was considered a side problem; nevertheless, it has recently come to the forefront of both the day-to-day operations of computer systems and networks, as well as the research conducted in Computer Science and Engineering. In point of fact, cyberattacks have a very substantial cost to the operations of systems, even when they are recognised and may be mitigated. This cost includes a degradation of the commercial image or trust, and the systems in question have to increase their running expenses.

Routing is the mechanism that is most responsible for maintaining the dependability of Internet access. As a result, it is always the target of cyberattacks; according to [1], only in 2017, around 14,000 cyberattacks, including hijacking, leaks, and spoofing, resulted in stolen data, lost money, and damaged reputations. Attacks on the transport service, attacks on the topology service, attacks on the route computation service, and attacks on the identity resolution service are all examples of routing attacks. These types of attacks are categorised in [2], and their purpose may be to exhaust network resources and deplete bandwidth, in addition to eavesdropping [3].

A large amount of research work is required to ensure that the route itself is secure (see [4]). The problem is present in mobile ad-hoc networks [5], but recently some works concerning security aware routing in SDN core networks have appeared [6]. Relatively less research activities are devoted to routing as a way of mitigating attacks. [5] However, the problem is present in mobile ad-hoc networks.

A. Background and outline of the Ser IoT Project

After conducting research into the potential role that routing could play in protecting computer networks from cyberattacks, we decided to make security-aware path management one of the primary focuses of the Secure and Safe Internet of Things (SerIoT) project [7],

which was recently granted funding by the European Commission. The SerIoT project was initiated in January of 2018, but its roots can be traced back to earlier research conducted over a decade ago on Distributed Denial of Service (DDoS) Attacks [8] and on utilising routing with the Cognitive Packet Network protocol (CPN) [9] to detect DDoS, and trace the attacking traffic so as to use CPN's ACK packets to drop the attacking traffic packets at upstream routers that carry the attacking traffic, and also detect worm attacks Additional information on the SerIoT may be found in references [11] and [12].

The Technical Objectives of the project include the means to comprehend the dangers that an economy built on the Internet of Things (IoT) faces, as well as the means to understand how distributed ledgers (Blockchain) may enhance IoT-based systems. Honeypots that are virtualized and self-aware will be designed and built by it in order to attract and analyse threats. Within the context of the project, a SerCPN network is being developed. This network will be responsible for the management of particular distributed IoT devices. It will also make use of the implementation of software-defined networks (SDN) that are based on CPN [13], and it will make use of measurements to generate system self-awareness [14]. These software-defined networks (SDNs) will make use of Cognitive Packets (CP) to search [16] for secure multi-hop routes having good quality of service (QoS) and measure their security and performance. Additionally, they will make use of Reinforcement Learning with Random Neural Networks (RNN) [17] to improve the network's overall performance, taking into account all three criteria of high security, good QoS, and low energy consumption [18]. Adaptive connections to Cloud and Fog servers [20] for the purpose of network data analysis and visualisation may be established between several SerCPN network clusters that are joined by means of an end overlay network [19]. The project will deliver a number of platforms that will comprise the main technical outputs of the project. These platforms will include: Platforms for I IoT Data Acquisition, Platforms for (ii) Ad-hoc Anomaly Detection, Platforms for (iii) Interactive Visual Analytics and Decision Support Tools, and Platforms for (iv) Mitigation and Counteraction, which will orchestrate, synchronise, and implement the decisions taken by the various components.

PROJECT OBJECTIVE – SECURITY AWARE ROUTING

One of the goals of the project is to design, implement, and test a secure network infrastructure for the Internet of Things (IoT) that is based on Software Defined Networks (SDN) and a smart SDN-Controller with online cognitive security surveillance and reporting, and with the ability to establish and dynamically modify paths to enhance security for IoT devices and end users, while offering a quasi-optimal level of quality of service (QoS) within the required security constraints. This will be accomplished The CPN (Cognitive Packet Network) paradigm, which was described in [21] and elaborated in [22], serves as the foundation for the online cognitive monitoring and path management of the network. [21] and [22] respectively. The implementation and performance of CPNs at the routing level has been detailed in a number of articles, including [16]. The usage of CPN as a software defined network (SDN) is explored in [23], while its implementation as an overlay network is discussed in [19]. The intelligent SDN network that will be developed as part of the SerIoT project and given the designation "SerIoT CPN network" or SerCPN begins with various ideas that are explored in [23].

The authors' work on a revolutionary approach to routing centres on the idea of confidence or trust as its central organising principle (the terms are used in-terchangeably). However, there are writers who have already defined trust in a form that is also utilised in the study, thus even if the concept can be deemed hazy in general, it is used in the paper. According to [24], the "degree of dependability" of the nodes in the network is the definition of trust. According to the definition that applies to our situation, we consider trust to be the probability that the cooperating nodes in the network will comply with the security policies that are enforced in the network and will not act in any malicious way to violence the security requirements of confidentiality, integrity, availability, authenticity, and non-repudiation. This definition is based on the context of our situation.

A. Design goals of SerCPN

The proposed SerCPN solution is a generic secure, QoS aware, and energy-conscious network solution. It is suited for usage in a variety of application settings, but in particular for the Internet of Things domain, where it may be utilised for applications such as the following:

1. IoT-centric virtual network, separated form operator’s backbone network.

2. Overlay over the Internet, where resources of public Internet are used in place of leased lines
3. Local communication within large IoT network

The traditional SDN methodology is utilised by SerCPN, which then expands upon it. It employs the OpenFlow protocol for communication between the data planes and the control planes of its design, which are isolated from one another. The following factors are considered while making decisions on the paths that data packets travel in the network, in the order of their importance:

1. Protection and safety first. The delivery of the data must be done in a dependable manner so as to reduce the possibility of it being stolen, lost (whether intentionally or by mistake), or intercepted.
2. The Standard of the Service A crucial factor to consider while selecting the channels for the delivery of packets, with regard to the Quality of Service parameters like as throughput, latency, and jitter.
3. Energy consumption. The load on the switches will be adjusted to use as little energy as possible, and the traffic will be spread across the various channels with the goal of reducing the amount of energy that is consumed by each packet or connection.

B. Routing Criteria

In the event of an implementation of SerCPN that is based on SDN, routing decisions are represented by the creation of relevant rules for the respective flows. An "oracle" will be responsible for making routing decisions. This "oracle" will be provided with data on security, quality of service, and energy, which will be saved in a cognitive security memory (CSM). In the same vein as CPN, the "oracle" will be realised through the utilisation of RNNs, which will especially take advantage of a real-time learning algorithm such as Reinforcement Learning (RL). The controller plugin is going to be updated to include RNNs. The data from the CSM will be utilised to provide quantitative measurements and evaluations for learning by the RNNs, and then sent to the analytics modules of SerIoT for exploitation. There are several strategies and techniques to traffic categorization and threat detection, some examples of which are [25] and [26], to name just a few. However, we are able to list an introduction list of activities, which will offer us a quantitative perspective at the degree of trust to network devices and network traffic. The choice of advanced threat detection

methods will be made in a later stage of the work.

1. An estimation of the level of security (trust) of devices that are linked to a certain SerIoT forwarder (SFE – see III) – the likelihood of the device being the attack's origin or target. This category contains verification tasks such as checking the default passwords, fingerprinting the firmware version, or doing automated active penetration testing on linked devices (one time or periodic).

2. The level of security (trust) of the SFEs, which refers to the likelihood that the node would be attacked and rendered inoperable or intercepted. Here, actions comparable to those in group 1 are taken into consideration, and additionally, we may use the availability rate of the nodes as a way to modify the trust level of a node. This would be independent of the reasons, such as attacks or technical failure, for which the availability rate of the nodes would be affected.

3. The safety (degree of confidence) of certain flows. We have a broad variety of approaches available here. Simple (lightweight) signals that a particular flow could be a part of an attack include protection that does not rely on statistics, such as the following examples:

- Checking if the source or destination of the flow is on the public blacklist of IP addresses,
- Detection of a bitrate exceeding predefined thresh- old,
- Detection of IP addresses scanning,
- Detection of non-standard use of protocols, etc.

At the end of the project we however intend to use also advanced techniques comparing traffic statistics with patterns of attacks using methods of mathematical statistics or artificial intelligence.

1. QoS parameters provided by particular paths. Through- put of given links, delay and jitter, as well as loss rates should be measured and forwarded to the CM.
2. Power consumption of particular nodes for specific mea- sured traffic values, achieved either by using a heuristic based on CPN [27] or by a computed optimization solution as in [28].

Thus the factors listed above in 1) through 5) will be used to create the Cognitive Goal Function [29] for SerCPN optimisation.

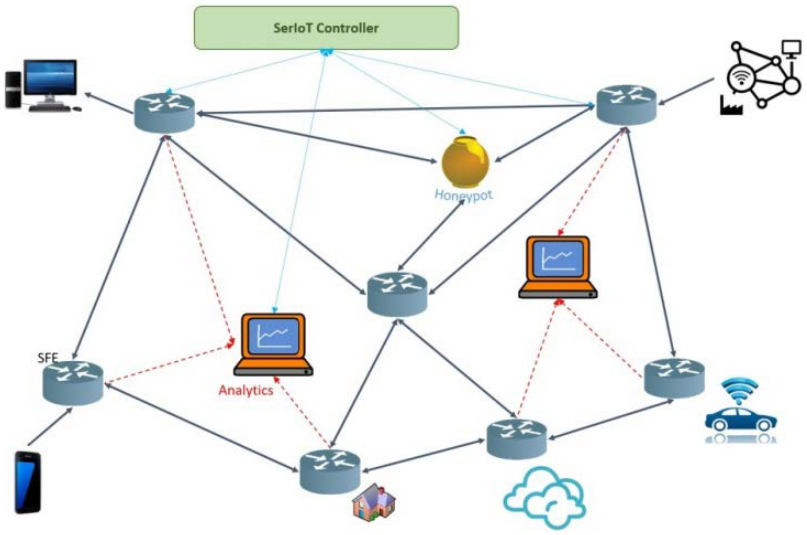

Figure: - 1 An example of a basic SerCPN network (single domain)

ARCHITECTURE OF THE SERCPN NETWORK

The routing methods that have been offered will be implemented as an extension of a traditional SDN network. We will implement new SerCPN components that are able to carry out the activities essential to accomplish the objectives of the project, particularly intelligent security aware routing. The following are some of the primary components of SerCPN:

1. SerCPN Forwarding Element (SFE),
2. SerCPN Controller(s),
3. SerIoT Analytics Module will exploit data collected by SerCPN,
4. SerIoT Honeypots will also attempt to attract attacks and inform SerCPN about the network state.

The Forwarding Element (SFE) of the SerCPN network is a fundamental component of the network. It is a Network Forwarding Element (NFE, often referred to inexactly as an SDN switch or SDN router) that has been updated specifically for the requirements of SerCPN. Regular packet switching is carried out by SFE in accordance with the requirements of OpenFlow. In addition, the SFE will utilise the CPNs strategy in order to carry out activities linked to the collection of data on energy consumption, quality of service, and security.

In addition to the SerCPN Routing Engine, the SerCPN controller will be a standard software-defined networking (SDN) controller (we picked ONOS – https://onosproject.org/) (SRE). The RNN-based Cognitive Routing Module is at the

centre of SRE and is responsible for making routing decisions. The purpose of the SerIoT Analytics Module (SAM) is to give an evaluation of the flows that are present in the SerCPN by doing statistical comparisons with the data from the past. Flows that exhibit features that are not consistent with the norm may be stopped, rerouted to a honeypot, or kept under observation for a decision to be made at a later time.

The SerIoT Honeypot (SH) is a system that is connected to SerCPN and analyses the assaults that are carried out on itself. It operates by imitating the operations of particular devices. It is possible for an adversary to gain control of it without causing any damage to other nodes in the SerCPN network.

IMPLEMENTATION OF DATA ACQUISITION AND ROUTING DECISIONS

The SerCPN Routing Engine (SRE) will be distributed in one or more SDN controllers as a plugin module. It will make use of the RNNs to implement the decision oracles, which will enable a semi-distributed method of making decisions while still making use of the benefits of the semi-centralization that is present in the SDN architecture. When particular RNNs are connected to specific SFEs, the resulting topology will reflect that of the physical network. Regarding a flow that is going to a certain location, it will be the responsibility of a single RNN to designate, at the time that decisions are being made, which output node should be utilised for a particular SFE. The SRE will collect data via utilising CPs and via controller, which will collect data from monitoring or analytical organisations.

The SerCPN makes use of CPs that move from one node to another on their way to their destination, during which time they collect measured data that is supplied by the nodes that they visit. In a typical scenario, the path of the CPs is supplied by the SFEs of the nodes that are traversed by the CPs, but the path of the ACKs is source routed from the destination node back to the source. Therefore, throughout the network, each of the nodes that was visited by a CP is able to receive and replicate the data that was gathered by a CP on its journey from the matching ACK (acknowledgement packets). This is possible because of how ACKs function. Such nodes are able to retain and make use of the information that has been gathered by each CP that has travelled to the node in question. The approach is modified in SerCPN because the sending of control

packets (CPs) and routing over the network are controlled by a controller and an SRE. Because of this, ACK packets, rather than travelling via the network using the route back to the source node, go to the SRE, which makes use of the content of the ACK packets to decide about routing.

CPs will be used for data that is not available otherwise, such as the delay on the link or the total delay between two adjacent nodes including the delay inside nodes, as well as for data that can be sent by nodes directly (asynchronously or by request), but which are less urgent. Examples of this type of data include the delay on the link or the total delay between two adjacent nodes, which includes the delay inside nodes (e.g. energy usage). CPs combine the information from several of the nodes along their journey into a single message before sending it back to the controller. This helps to reduce any potential communication overhead.

REAL LIFE EVALUATION

The outputs of the SerIoT project will be assessed based on their applicability to a variety of key real-world use cases. These are broken down into four primary categories. The first one is called "Surveillance," and it refers to a system that will monitor the actual safety of bus depots using the infrastructure of OASA, which is the most important transportation body in Greece. The second one has to do with Intelligent Transport Systems in Smart Cities, and we will show how SerIoT may improve the cyber security of such systems so that vehicles are safer. The third use case will involve Flexible Manufacturing Systems (Industry 4.0), which, with the assistance of Deutsche Telekom/T-Sys., will monitor physical attacks to wireless sensor networks. This will be done for situations relating to automated warehouses, in which different attack vectors may be used for breaking or jamming communication lines. The fourth use case will deal with Food Chains, which call for end-to-end security through multiple communication channels. This security must include device authentication, the detection and avoidance of DDoS and replication attacks, as well as the detection of functionality anomalies and the disabling of IoT devices.

Therefore, the confrontation in SerIoT of the physical world with issues of cybersecurity creates a rich opportunity to move forward from the traditional work in this field that focuses on cryptography and the management of cryptographic keys [30], [31], or the security of software [32] and physical structures [33], to broad

issues regarding security and system efficiency in the presence of cyberattacks to the integrated cyber and physical infrastructure.

CONCLUSIONS

The primary objective of the SerIoT project is to improve the information and data security of Internet of Things platforms and networks in a manner that is holistic and cross-layered. The duration of the SerIoT project is anticipated to be three years. The efforts that were made during the present time period (the first year) were concentrated on what is known as "Framework Design and Preparation" for Phase 1. Following the completion of the exhaustive examination of use case scenarios, the requirements for the system were defined. Both the formal and functional specifications of the individual components of the framework, as well as the overall architecture of the framework, have been developed.

In the paper, which the authors contributed to the SerIoT project, the primary emphasis is placed on novel multi-criterion routing for the SDN-based architecture. This routing is not only security-aware; it also includes QoS and energy awareness rules, and it makes use of RNNs to accomplish its objectives. In the section devoted to security, we will investigate the idea of having confidence with regard to certain devices and network flows. This will be done on the basis of measures that are obtainable in an SDN network. The characteristics of network traffic generated by IoT devices will make it possible for us to define risks and symptoms of malicious behaviour with greater precision than in networks of a general nature, and a dedicated module that processes security-related information gathered from a variety of sources can be modified to accommodate new threats and attack vectors. The integration of all of the project's components, as well as the deployment of the testbed and the test plan, is going to be the next hurdle the project faces.

REFERENCES

1. M. Siavvas, E. Gelenbe, D. Kehagias, and D. Tzovaras, “Static analysis- based approaches for secure software development,” in Proceedings of the 2018 ISCIS Security Workshop: Recent Cybersecurity Research in Europe (E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, eds.),

vol. 821, Lecture Notes CCIS, Springer Verlag, 2018.

2. A. Herzberg, M. Hollick, and A. Perrig, “Secure Routing for Future Communication Networks (Dagstuhl Seminar 15102),” Dagstuhl Re- ports, vol. 5, no. 3, pp. 28–40, 2015.

3. E. Hanselman, “Manrs project study report,” tech. rep., 451 Research, Commissioned by Internet Society, August 2017.

4. M. Wang, J. Liu, J. Mao, H. Cheng, J. Chen, and C. Qi, “RouteGuardian: Constructing Secure Routing Paths in Software-Defined Networking,” Tsinghua Science and Technology, vol. 4, no. 22, pp. 400–412, 2017.

5. F. Franc¸ois and E. Gelenbe, “Towards a cognitive routing engine for software defined networks,” in ICC 2016, pp. 1–6, IEEE Xplore, 2016.

6. A. Levi, M. U. C¸ aglayan, and C¸ . K. Koc¸, “Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure,” ACM Trans. Inf. Syst. Secur., vol. 7, no. 1, pp. 21–59, 2004.

7. E. Gelenbe, “Steps toward self-aware networks,” Communications of the ACM, vol. 52, no. 7, pp. 66–75, 2009.

8. E. Gelenbe, “Cognitive packet network,” US Patent 6,804,201, 2004.

9. S. Devisri and C. Balasubramaniam, “Secure routing using trust based mechanism in wireless sensor networks(wsns),” International Journal of Scientific & Engineering Research, vol. 4, 2013.

10. C. Yu, G. Ni, I. Chen, E. Gelenbe, and S. Kuo, “Top-k query result completeness verification in tiered sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 109–124, 2014.

11. P. Foremski, C. Callegari, and M. Pagano, “Waterfall: Rapid identifica- tion of ip flows using cascade classification,” in

International Conference on Computer Networks, pp. 14–23, Springer, 2014.

12. E. Gelenbe, “Dealing with software viruses: a biological paradigm,” information security technical report, vol. 12, no. 4, pp. 242–250, 2007.

13. J. Doman´ska, M. Nowak, S. Nowak, and T. Czacho´rski, “European cy- bersecurity research and the seriot project,” in Computer and Information Sciences (T. Czacho´rski, E. Gelenbe, K. Grochla, and R. Lent, eds.), (Cham), pp. 166–173, Springer International Publishing, 2018.

14. E. Gelenbe and H. Bi, “Emergency navigation without an infrastructure,” Sensors, vol. 14, no. 8, pp. 15142–15162, 2014.