Cognitive Packet Networks for the Secure Internet of Things

Mateusz Nowak, Sławomir Nowak, Joanna Domańska, Tadeusz Czachórski
Institute of Theoretical and Applied Informatics, PAS
Gliwice, Poland
{mateusz,snowak,joanna,tadek}@iitis.pl

***Abstract*—The concept of Security Aware Routing is not widely adopted in current networks. However, the new IoT-centric core networks give possibilities to re-open that field of research. We consider routing to be an addition to existing network security methods, especially in IoT domain. Security-aware routing incorporates the security and safety metrics to the traditional set of metrics (bandwidth, network delay, hop count, path cost, load etc.). The paper shows a new approach in which, based on the Software Defined Networks (SDN) we estimate trust relationships between nodes and flows and use them to create SDN paths, based on the Cognitive Packet Network (CPN) principle. The Random Neural Networks (RNN) supported with cognitive packets are used for making routing decisions. The proposed solution was designed and is being implemented within the SerIoT project to demonstrate secure networks for the Internet of Things (IoT).**

***Index Terms*—Internet of Things (IoT), Security, SDN, Random Neural Networks, Energy, Cognitive Packet Network, SerIoT**

I. Introduction

Internet of Things (IoT) is the area of computer networks through which the most sensitive data are transmitted, including the privacy (eg. localisation tracking or health data) or business-critical data. Cybersecurity in IoT had been viewed as a peripheral issue for a long time, but now it moved to the forefront of everyday computer system and network operations, and of research in Computer Science and Engineering. Indeed cyberattacks, even when they are detected and mitigated, have a very large cost to systems operations including the degradation of the commercial image or trust and have to increase their operating costs.

The key process ensuring reliability of Internet connectivity is routing. Therefore it is continuously the aim of cyber-attacks - according to [1] only in 2017 ca. 14,000 attacks such as hijacking, leaks, spoofing led to data deft, revenue lost and reputation damage. Attacks on the transport service, attacks on the topology service, attacks on the route computation service and attacks on the identity resolution service are categories of routing attacks, classified in [2], and their purpose may be exhausting network resources and deplete bandwidth, and also eavesdropping [3]. Securing the routing itself is a matter of significant research effort (see [4]). Relatively less research activities is devoted to routing as a way of attacks mitigation – the problem is present in mobile ad-hoc networks [5], but recently some works concerning security aware routing in SDN core networks appeared [6].

A. Background and outline of the SerIoT Project

Exploring possible role of routing as a way of counteracting cyberattacks in computer networks made us to set security-aware path management as one of important goals of the Secure and Safe Internet of Things (SerIoT) project [7] accepted for funding by European Commission. The SerIoT project started in January of 2018, but finds its origins in early work started over a decade ago on Distributed Denial of Service (DDoS) Attacks [8] and on using 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 [10]. Further details regarding SerIoT can also be found in [11], [12]. The project's Technical Objectives include means to understand the threats to a IoT based economy and understand how distributed ledgers (Blockchain) may improve IoT based systems. It will design and implement virtualised self-aware honeypots to attract and analyse attacks.

Within the project the SerCPN network is designed, that manages specific distributed IoT devices and will use the implementation of Software Defined Networks (SDN) based on CPN [13] using measurements that create the system self-awareness [14]. These SDNs will use Cognitive Packets (CP) to search [16] for secure multi-hop routes having good quality of service (QoS) and measure their security and performance, and will use Reinforcement Learning with Random Neural Networks (RNN) [17] to improve the network overall performance, including all three criteria of high security, good QoS and low energy consumption [18]. Several SerCPN network clusters may be interconnected via end overlay network [19], with adaptive connections to Cloud and Fog servers [20] for network data analysis and visualisation.

The project will deliver a number of platforms that comprise the main technical outputs of the project, including Platforms for (i) IoT Data Acquisition, (ii) Ad-hoc Anomaly Detection, (iii) Interactive Visual Analytics and Decision Support Tools, and (iv) Mitigation and Counteraction that will orchestrate,

The authors gratefully acknowledge the support of the SerIoT Research and Innovation Action, funded by the European Commission under the H2020-IOT-2017 Program through Grant Agreement 780139.

978-1-7281-2171-0/19/$31.00 © 2019 IEEE

synchronise and implement the decisions taken by the various components.

II. Project objective – Security Aware Routing

One of the objectives of the project is to design, implement and test a secure network infrastructure for the IoT, 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. The online cognitive surveillance and path management of the network is based on the CPN (Cognitive Packet Network) principle that was discussed in [21] and detailed in [22]. CPNs routing level implementation and performance is presented in various papers such as [16]. CPN's implementation as an overlay network is discussed in [19], and its use as a software defined network (SDN) is discussed in [23]. The smart SDN network designated "SerIoT CPN network" or SerCPN that we will develop in the SerIoT project, starts with some designs discussed in [23].

The key concept used in the authors' work on novel approach to routing is confidence or trust (the terms are used interchangeably). In general the term might be considered vague, still, there are authors who already defined trust in a way which is also used in the paper. In [24] trust is defined as the ”degree of reliability" of nodes in the network. Following the definition in our context, we consider trust as the probability that the cooperating nodes in the network will comply with the security policies 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.

A. Design goals of SerCPN

The proposed SerCPN solution is a general secure, QoS aware and energy-aware network solution, suitable for use in various application contexts, and in particular for the IoT domain, such as:

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

SerCPN utilises and extends the classic SDN approach. It has an architecture of separated data and control planes, and uses the OpenFlow protocol for communication between them. Decisions about the routes the packets move are made according to the following criteria, ordered by priority:

1) **Security and Safety.** Data must be delivered in reliable way, minimizing the risk of being lost (due to intended attack or accidental failure) or intercepted.
2) **Quality of Service**. An important criterion for choosing the paths for packet delivery respecting the QoS parameters such as throughput, delay and jitter.
3) **Energy usage**. The load of switches will be adjusted to minimise energy usage, while traffic will be distributed on paths with a view to minimizing the energy consumption per packet or per connection.

B. Routing Criteria

In the case of a SDN based implementation for SerCPN, routing decisions are reflected by creating appropriate rules for given flows. The routing decisions will be taken by an "oracle", which is fed with security, QoS and energy data, which will be stored in a Cognitive Security Memory (CSM). As in CPN the "oracle" will be implemented using RNNs which will specifically exploit a real-time learning algorithm such as Reinforcement Learning (RL). RNNs will be placed in the controller plugin. The CSM data will be used providing quantitative metrics and evaluations for learning by the RNNs, and transferred for exploitation by the analytics modules of SerIoT. There exist many methods and approaches to traffic classification and threats detection, eg. [25] or [26] to list just few. The choice of advanced threats detection methods will be done in later stage of the work, however we can list introductory list of actions, which will give us quantitative view at level of trust to network devices and network traffic.

1) Estimation of security (trust level) of devices connected to given SerIoT forwarder (SFE – see III) – likeliness of being the source or destination of the attack. This group includes verifications actions such as the verification of default credentials, the fingerprinting the firmware version, or automatic active penetration testing of connected devices (one time or periodic).
2) Security (trust level) of the SFEs – likeliness of the node being attacked and disabled or intercepted. Actions similar to group 1 are considered here, as well as we may use the availability rate of the nodes, independently of the reasons such as attacks or technical failure, as a way to modify the trust level of a node.
3) Security (trust level) of particular flows. Here we have a wide group of methods. Simple (lightweight) indications that a given flow maight be a part of an attack include prevention without using statistics, e.g.:
   - Checking if the source or destination of the flow is on the public blacklist of IP addresses,
   - Detection of a bitrate exceeding predefined threshold,
   - 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.
4) QoS parameters provided by particular paths. Throughput of given links, delay and jitter, as well as loss rates should be measured and forwarded to the CM.
5) Power consumption of particular nodes for specific measured traffic values, achieved either by using a heuristic

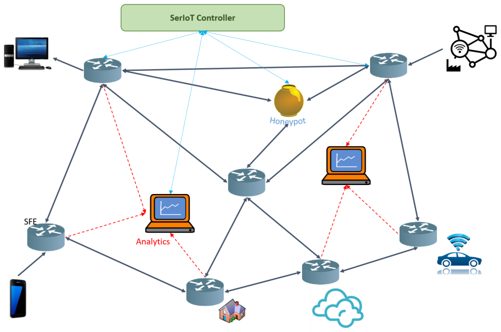

Fig. 1. An example of a basic SerCPN network (single domain)

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.

III. Architecture of the SerCPN network

The proposed routing solutions will be implemented as extension of classic SDN network. We will introduce new SerCPN's components, able to perform actions necessary to reach the project's goals, especially smart security aware routing. Main components of SerCPN include:

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.

SerCPN's Forwarding Element (SFE) is a basic component of the network. It is a Network Forwarding Element (NFE, referred often imprecisely as SDN switch or SDN router) modified for the needs of SerCPN. SFE performs regular packet switching according to OpenFlow rules. In addition, SFE will use the CPNs approach to perform tasks related to gathering security, QoS and energy usage data.

The SerCPN controller will be standard SDN controller (we chose ONOS – https://onosproject.org/), accompanied by SerCPN Routing Engine (SRE). Heart of SRE is RNN-based Cognitive Routing Module taking the routing decisions. The aim of the **SerIoT Analytics Module** (SAM) is to provide evaluation of flows in the SerCPN by statistical comparison with historical data. Flows having characteristics different than expected may be blocked, or directed towards a Honeypot, or put under observation for a later decision.

The SerIoT Honeypot (SH) is a system which mimics the functions of certain devices; it is connected to SerCPN and analyzes the attacks that are conducted on itself. It can be taken over by an attacker without any harm to other nodes of SerCPN.

IV. 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, using the RNNs to implement the decision oracles, enabling a semi-distributed way of taking decisions, but using the advantages of the semi-centralisation of the SDN architecture. Linking specific RNNs to SFEs will reflect the physical network topology. The role of a single RNN will be to specify, at the time of decision making, which output node should be used for a given SFE, regarding a flow having a given destination. Data will be gathered by the SRE using CPs and via controller, which gathers data from monitoring or analytic entities.

The SerCPN uses CPs that travel from one node to another towards their destination, gathering measured data that is provided by the nodes that are visited. Normally, the path of the CPs is provided by the SFEs of the nodes visited by the CPs, and the path of ACKs is source routed from the destination node back to the source. Thus in the network each of the nodes visited by a CP is able to receive and copy from the corresponding ACK (acknowledgement packets) the data that was collected by a CP on its path. Such nodes can then store and exploit the data that has been collected by each CP that visited the node. In SerCPN the approach is modified, as sending of CPs and routing over the network is controlled by a controller and SRE, so ACK packets, instead of travelling via the network using the route back to the source node, go to the SRE, which makes use if their content to decide about routing.

CPs will be used for data which is not available otherwise, such as delay on the link or total delay between two adjacent nodes including the delay inside nodes, and for data which can be sent by nodes directly (asynchronously or by request) but which are less urgent (e.g. energy usage). CPs aggregate the data from many nodes on their path and send them back to controller in a single message, reducing the potential communication overhead.

V. Real life evaluation

The SerIoT project's outcomes will be evaluated in a number of significant real-life use cases. These include four main areas. The first one is Surveillance, where physical security in bus depots will be monitored through the infrastructure of OASA, the largest transport authority in Greece. The second one involves Intelligent Transport Systems in Smart Cities, where we will demonstrate how SerIoT can enhance the cyber-security of such systems for vehicle safety. The third use case will involve Flexible Manufacturing Systems (Industry 4.0), which will monitor physical attacks to wireless sensor networks with the help of Deutsche Telekom/T-Sys., for situations related to automated warehouses where different attack vectors may be used for breaking or jamming communication lines. The fourth use case will address Food Chains which require end-to-end security through multiple communication channels, including device authentication, detection and avoidance of

DDoS and replication attacks, and detection of functionality anomalies and disabling of IoT devices.

Thus the confrontation in SerIoT of the physical world with issues of cybersecurity, creates a rich opportunity to move forward from traditional work in this area 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.

VI. Conclusions

The main goal of the SerIoT project is to optimize information and data security in IoT plat-forms and networks in a holistic, cross-layered manner. The SerIoT project is scheduled for three years. The effort in the current period (first year) was focused on the so-called Phase 1 "Framework Design and Preparation". The extensive analysis of use case scenarios were performed and the requirements for the system were formulated. The overall architecture of the framework was prepared as well as formal and functional specification of components.

The main focus of mechanisms presented in the paper, contributed by authors to SerIoT project, is at novel multicriteria routing for the SDN-based architecture, not only security-aware, but also including QoS and energy awareness rules, and using RNNs to achieve the goals. The security part will explore the concept of confidence to particular devices and network flows, based on measurements which are achievable in SDN network. The characteristics of network traffic from IoT devices will enable us to define risks and symptoms of malicious behaviour more precisely than in network of a general nature, and the dedicated module processing the security-related information from various sources can be adapted to new threats and attack vectors. The upcoming challenge for the project will be the integration of all components, deployment of the testbed and the test plan.

References

[1] E. Hanselman, "Manrs project study report," tech. rep., 451 Research, Commissioned by Internet Society, August 2017.

[2] M. Hollick, C. Nita-Rotaru, and P. Papadimitratos, "Toward a taxonomy and attacker model for secure routing protocols," *ACM SIGCOMM Computer Communication Review*, vol. 47, 2017.

[3] E. B. Eskca, O. Abuzaghleh, P. Joshi, S. Bondugula, and T. Nakayama, "Software defined networks security: An analysis of issues and solutions," *International Journal of Scientific & Engineering Research*, vol. 6, 2015.

[4] A. Herzberg, M. Hollick, and A. Perrig, "Secure Routing for Future Communication Networks (Dagstuhl Seminar 15102)," *Dagstuhl Reports*, vol. 5, no. 3, pp. 28–40, 2015.

[5] P. Lokulwar, V. Shelkhe, and M. Ghonge, *Security Aware Routing Protocol for Manet*. LAP Lambert Academic Publishing, 2012.

[6] 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.

[7] J. Domanska, E. Gelenbe, T. Czachorski, A. Drosou, and D. Tzovaras, "Research and innovation action for the security of the internet of things: The seriot project," in *Recent Cybersecurity Research in Europe, EURO Cybersec 2018* (E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, eds.), Lecture Notes CCIS No. 821, Springer Verlag, 2018.

[8] E. Gelenbe, "Dealing with software viruses: a biological paradigm," *information security technical report*, vol. 12, no. 4, pp. 242–250, 2007.

[9] E. Gelenbe, R. Lent, and A. Nunez, "Self-aware networks and qos," *Proceedings of the IEEE*, vol. 92, no. 9, pp. 1478–1489, 2004.

[10] G. Sakellari and E. Gelenbe, "Demonstrating cognitive packet network resilience to worm attacks," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 636–638, ACM, 2010.

[11] E. Gelenbe, J. Domanska, T. Czachorski, A. Drosou, and D. Tzovaras, "Security for internet of things: The seriot project," in *International Symposium on Networks, Computers and Communications, Proceedings of the*, IEEE, June 2018.

[12] J. Domańska, M. Nowak, S. Nowak, and T. Czachórski, "European cybersecurity research and the seriot project," in *Computer and Information Sciences* (T. Czachórski, E. Gelenbe, K. Grochla, and R. Lent, eds.), (Cham), pp. 166–173, Springer International Publishing, 2018.

[13] F. François and E. Gelenbe, "Optimizing secure sdn-enabled inter-data centre overlay networks through cognitive routing," in *24th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, MASCOTS 2016, London, United Kingdom, September 19-21, 2016*, pp. 283–288, 2016.

[14] E. Gelenbe, R. Lent, and Z. Xu, "Measurement and performance of a cognitive packet network," *Computer Networks*, vol. 37, no. 6, pp. 691–701, 2001.

[15] E. Gelenbe, "Steps toward self-aware networks," *Communications of the ACM*, vol. 52, no. 7, pp. 66–75, 2009.

[16] E. Gelenbe, "Random neural networks with negative and positive signals and product form solution," *Neural Computation*, vol. 1, no. 4, pp. 502–510, 1989.

[17] E. Gelenbe and R. Lent, "Power-aware ad hoc cognitive packet networks," *Ad Hoc Networks*, vol. 2, no. 3, pp. 205–216, 2004.

[18] O. Brun, L. Wang, and E. Gelenbe, "Big data for autonomic intercontinental communications," *IEEE Transactions on Selected Areas in Communications*, vol. 34, no. 3, pp. 575–583, 2016.

[19] L. Wang, O. Brun, and E. Gelenbe, "Adaptive workload distribution for local and remote clouds," in *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on*, pp. 003984–003988, IEEE, 2016.

[20] E. Gelenbe, Z. Xu, and E. Seref, "Cognitive packet networks," in *Tools with Artificial Intelligence 1999. Proceedings. 11th IEEE International Conference on*, pp. 47–54, 1999.

[21] E. Gelenbe, "Cognitive packet network," *US Patent 6,804,201*, 2004.

[22] F. François and E. Gelenbe, "Towards a cognitive routing engine for software defined networks," in *ICC 2016*, pp. 1–6, IEEE Xplore, 2016.

[23] 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.

[24] M. Min, L. Xiao, C. Xie, M. Hajimirsadeghi, and N. B. Mandayam, "Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach," *CoRR*, vol. abs/1801.06270, 2018.

[25] P. Foremski, C. Callegari, and M. Pagano, "Waterfall: Rapid identification of ip flows using cascade classification," in *International Conference on Computer Networks*, pp. 14–23, Springer, 2014.

[26] E. Gelenbe and T. Mahmoodi, "Energy-aware routing in the cognitive packet network," in *ENERGY*, pp. 7–12, 2011.

[27] E. Gelenbe and C. Morfopoulou, "A framework for energy-aware routing in packet networks," *Computer Journal*, vol. 54, no. 6, pp. 850–859, 2011.

[28] E. Gelenbe, "Steps toward self-aware networks," *Commun. ACM*, vol. 52, no. 7, pp. 66–75, 2009.

[29] A. Levi, M. U. Çaglayan, and Ç. K. Koç, "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.

[30] 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.

[31] 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.

[32] E. Gelenbe and H. Bi, "Emergency navigation without an infrastructure," *Sensors*, vol. 14, no. 8, pp. 15142–15162, 2014.