SDN Based Security in Mobile Ad hoc Networks

Nada Mouchfiq, Ahmed Habbani, and Chaimae Benjbara

***Abstract*—Current research is focused on wireless networks, more recently the Internet of Things and the ad hoc networks that are part of it. The combination of these networks and emerging technologies has identified the concept of the digital environment that has changed people's lifestyles and led to the emergence of new applied sciences. With the evolution that the world has experienced following the emergence of several concepts and the rapid development of technologies, security has become increasingly important must identify the different changes in the digital environment, namely data protection personal and professional. In the literature, there are several methods and levels of security. This article will discuss attacks that affect MANETs layers. Then we will discuss the proposed solutions to ensure a high level of security in these networks recalling the last work of our team, finally our article will propose a method of security the most adapted to our needs as a team and this method is based on the principle Software Defined Networks (SDN) that will be applied on MANETs (Mobile ad hoc networks).**

***Index Terms*—Attacks, IoT, MANETs, SDN, security.**

I. Introduction

The Internet of things refers to a type of network to connect anything with the Internet [1]. The concept of the Internet of Things has become a generic term for many technologies in order to improve the efficiency of the future cities and the quality of life of their inhabitants, not only by introducing new applications but also by making existing smarter processes that make life easier and more peaceful for individuals. It has become a trend to talk about IOT and there are efforts being made by several countries to develop this.

IoT environment is composed of different networks (Cloud, Big Data, Industry 4.0,..) among them, we find ad hoc networks that are several types: MANETs, VANETs, FANETs ...Each network has his own challenges, ad hoc networks can face several challenges including: Routing and multicasting, Quality of service, Energy, Security, Mobility…

MANETs are a system of mobile nodes connected with each other via wireless links without infrastructure support [2]. The figure below shows the exact classification of the MANETS networks architecture [3] based on the OSI model.

The dynamic appearance of MANETs makes them vulnerable to multiple attacks, so many threats can harm the MANETs networks. In the following table we can find various attacks in each of the 5 layers in the MANETs [4].

Manuscript received March 26, 2020; revised June 5, 2020.

All authors are with ENSIAS, Mohamed 5 University, Rabat, Morocco (e-mail: mouchfiq.nada@gmail.com, habbani@ifride.com, benjbara@ifride.com).

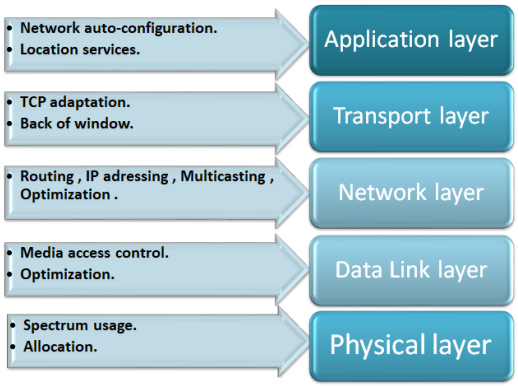

Fig. 1. MANETs architecture.

TABLE I: MANETs Threats

Layers	Attacks
Application Layer	• Repudiation • Malicious Code
Transport Layer	• Session Hijacking • SYN flooding
Network Layer	• Black hole • Gray hole • Wormhole • Information disclosure • Message altering • Sending data to node out • Transmission range • Routing attacks
Data Link Layer	• Jamming • Selfish misbehavior of nodes • Malicious behavior of nodes • Traffic Analysis
Physical Layer	• Eavesdropping • Active interference • Jamming

Several studies have proposed solutions to solve safety problems that harm MANETs [5]:

1) Cluster-based intrusion detection technique.
2) Misbehavior detection through cross-layer analysis.
3) Defense method against wormhole attacks.
4) Defense mechanism against rushing attacks.

There are other more relevant solutions applied in other areas such as the SDN (Software Defined Networking) which makes the network more secure and flexible, [6] its principle is then based on the separation of the routing plan from that of the control and on giving orders to the control plane from the API (Application Programming Interface) via applications [7]. There are two SDN models:

1) Programmability via a controller: In this model, an application gives an abstract and global order to a controller, which transmits this in parts to other network devices.
2) SDN Overlay: which consists of creating a virtual environment whose mission is to ensure connectivity between nodes.

doi: 10.18178/jacn.2020.8.1.277

The remainder of the paper is organized as follows: Section II: Related Work, Section III: Our proposition and we will finish with the conclusion in Section IV.

II. Related Work

A. Encryption-Based Solutions

The researchers deployed several measures to address security issues in each layer of the IoT framework, one of them proposed a hybrid encryption technique (cryptographic paradigm) highlighting both the symmetrical key advantage and the asymmetric key performance for IoT security. The approach deals with securing the IoT application layer to ensure security measures, namely: integrity of information, confidentiality, non-repudiation data transmitted in IoT using a mixed encryption algorithm [8]; used to encrypt data and as a cryptographic signature he proposed the elliptic curve cryptography algorithm.

Another proposal is in the form of a protocol that combines evidence and key exchange mechanisms to provide secure and authenticated communication in networks. The protocol requires prior knowledge of network configuration and structure, and guarantees perfect transmission [9].

Another implementation is the use of encryption security certificate. The certificate provides a method of once a encrypt between communicating parts (sensor nodes in IoT). It uses a lightweight encryption or decryption method that uses timestamp technology so that speed and communication between the nodes are guaranteed [10].

A similar approach was used to detect malware USB devices forces a USB drive that is plugged to undergo a series of virus scans before being done available to the user or any other part of the system [11]. The system obviously differs in that we are concerned with the network access rather than automatic execution of malware but also in that we also focus on healing vulnerabilities and providing useful information to the user.

B. SDN Security and Energy Efficiency

In this work, [12] they proposed an architecture for the SDN by shedding light on the operation of each of its components, and they also summarized the recent security attacks and countermeasures in SDN, the old and new ones, they also implemented the software defined network (SDN) capability to deal with multiple attacks as well as energy efficiency. They also provided strategies for achieving energy efficiency in the networks through the SDN.

In Fig. 2, they gave the evolution of the energy consumption of a traditional network and an SDN network SDN for different sizes of data. Although the variation of the consumption in terms of energy increases for both networks, but for the SDN network, it consumes energy near to that of the traditional network only when it uses its maximum speed and implements its link thoroughly. And since the SDN can adapt its parameters according to the size of the information to be sent, so it is able to consume minimal energy without affecting the performance of the network in its entirety.

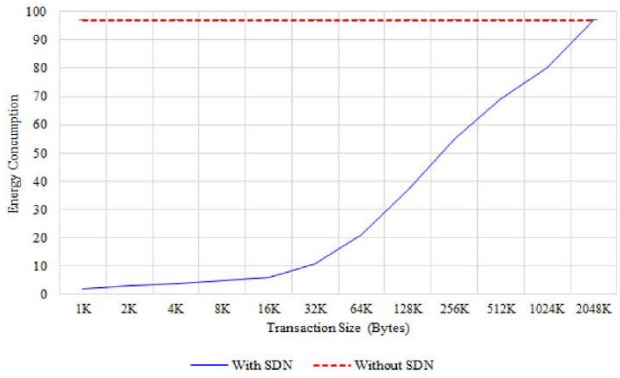

Fig. 2. Comparison of energy consumption for SSL handshake with and without SDN implementation with increasing transaction sizes.

C. SDN Framework for Securing IoT Networks

The principle of this model [13] allows the data of the IoT layer to be transmitted in an elitist way via the main framework of the SDN layer, and in which the essential functions of analysis of the security (control of access ... etc) are put in place, which makes it possible to bridge the separation which could exist between the IoT networks and the usual computer networks. This approach consists of integrating a monitoring mechanism that takes into account:

1) Optimization on several levels namely: security analysis dynamics, memory dedicated to metadata, control protocols load ...
2) The minimization of transmission delay of the packets through the distinction of the attacks.

The accuracy of the detection of the packets which tend to harm the system. The authors of the accepted manuscripts will be given a copyright form and the form should accompany your final submission.

The integrated IoT in this network framework as shown in the figure below takes a heterogeneous aspect by the presence of physical and communication devices using unique identifiers and interconnected objects using protocol. This improves the notion of ubiquitous computing compared to the latest technology in the form of the Internet of Things. These objects allow the Internet connection to work anytime, anywhere.

This approach has highlighted the potential of the SDN and its capabilities such a engineering and monitoring the dynamic application of policies, access control at the time of device mobility, which is considered a gain to overcome security challenges in such networks as SDN integration brings dynamism and flexibility to the network.

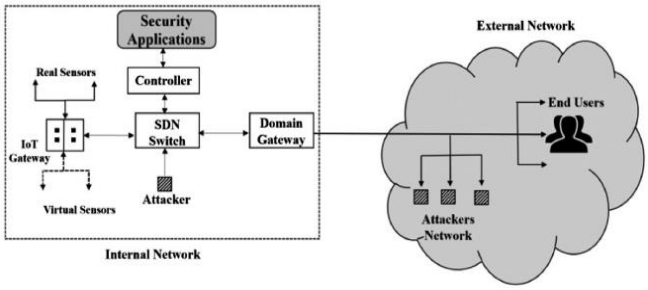

Fig. 3. Experimental network topology.

The proposed architecture in the figure above of this model is divided into two parts, an internal network and an external

network:

Internal network:

1) Edge Domain Gateway, a linux intrusion detection system (SNORT / IDS (Intrusion Detection System))
2) SDN stack: RYU controller management, modified security / attack detection, modified Switching Software (OVS (Open VSwitch)).
3) IoT stack: Gateway under ContikiOS, which supports almost 6 network protocols, in which SDN Open Flow is activated.
4) IoT sensor network: consists of 4 to 6 physical sensors whose virtual simulation is carried out by 2 workstations.
5) IoT Attack: This is a software-based simulation system that generates malware traffic and jamming protocols.
6) General internal attacks: in which they use machines which in turn execute the operating assortments.

External network:

1) Configuring legal hosts that use protocols (TCP / IP, MQTT) to access the IoT test network.
2) Attack host users, and design denial of service attacks and targeted attacks that harm the system by embedding malicious software as an example.

D. Security-Based Mechanism for Proactive Routing Schema Using Game Theory Models

Our team (M3S: Mobile Smart Security Systems) works on ad hoc networks, more specifically ad hoc mobile networks (MANETs) which are wireless networks with mobile components without infrastructure and which make the configuration in a continuous way. Each component of MANETs has the possibility to move freely in the network and must each time have traffic related to its use [14]. This is the reason why MANETs nodes act both as a router and as a host. Challenges for MANETs include: dynamic topologies, mobility, energy, speed, quality of service and security, encountered at different levels of MANETs.

These challenges are being researched by the members of the team I work with. A colleague [15] worked on ”Security-based mechanism for proactive routing scheme using a game theory model”, he was able to improve the security aspect of MANET networks by reducing the effect of malicious nodes in the network because this solution allows each node to know the behavior of other nodes and make it possible for smart nodes to choose strategies to deal with ego nodes , and this while retaining residual energy benefits, the average end time end and packets exchanged within the network.

Energy impact: We noticed that malicious nodes are able to save energy when they refuse to cooperate for routing packets. Therefore, rational nodes must make more effort to compensate for the non-cooperation of malicious nodes and therefore expend more energy to accomplish this task.

End to end delay impact : This proposal can offer almost the same result compared to the original OLSR, and in terms of the impact of a packet collision, noise transmission and processing time needed to calculate the CR (Carriage return), our solution provides an ETED (End To End Delay) that is less effective than the original OLSR.

Exchanged packets impact: The number of packets exchanged is high in original OLSR and enhanced OLSR in comparison with those exchanged with selfish OLSR.
This is due to the fact that malicious nodes choose to drop rather the received packets than to transfer them to their destinations.

Therefore, the behavior of malicious nodes should influence the number of packets received since they do not. In addition, the results obtained in this work support the effectiveness of the proposal using a malicious node detection mechanism.

III. Our Proposition

Software defined networking (SDN) should be a key tool for later generation networks called 5G (5th Generation Wireless Systems), which will need to integrate both IoT services as well as traditional human-based services. In this context, SDN enables full harmonization of distributed cloud, heterogeneous networks and IoT resources needed to:

1) Wirelessly transport the huge amount of data generated by terminals, sensors, machines, nodes, etc., to any distributed node, edge, or central data center.
2) Free space for IT, storage and network.
3) Process the absorbed data (Big Data).
4) take the most correct choices (cognition).

One of the biggest challenges which present IoT and implicitly MANETs to network administrators is the ability to collect data and conduct analysis to produce a positive user experience on the go. SDN is able to redirect traffic automatically when needed, which significantly improves the IoT applications. Through orchestration virtual network, storage and computing resources are provisioned and instantly delivered for the analysis of data. However, due to the fact that untrusted IoT devices might be interconnected towards the aggregation networks or external malware could be applied to the network security issues may arise. It is in this context, SDN can offer a plethora of solutions to enhance security The challenges of IOT that SDN can solve:

1) SDN automation reaches the Internet of Things (IOT).
2) SDN can spread a scalable distributed system to handle the flow of events.
3) SDN can provide the frictionless integration of new IoT components designed and deployed by multiple vendors in distributed systems and various data streams in a scalable way and produce it in an expected effect. What primitives does a network need to experience the diversity of protocols in IoT.

According to our research, it has been found that there are new security approaches applied in other networks such as the SDN in IoT we have mentioned in our article. It has therefore been proposed to apply the principle of SDN security in ad hoc networks in order to see its impact on the degree of security that it will offer to our MANETs network by preserving the metrics mentioned above (residual energy, the average end-to-end time and the packets exchanged within the network).

In order to ensure the continuity of teamwork and especially to ensure network security by using the improved OLSR protocols developed in our team, we propose a security method more adapted to our needs and to the intelligent systems to which we are interested and to keep to the maximum the performances of the system, this method is

based on the principle of the SDN.

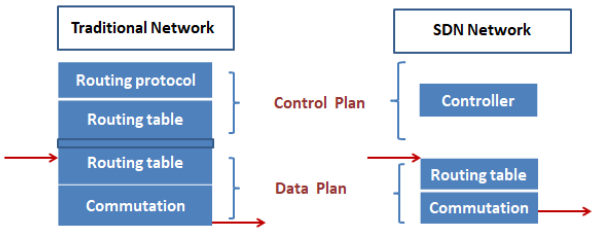

Fig. 4. Traditional network vs SDN network.

Indeed, as shown in the figure above, the traditional networks distribute the control plane, they are static networks that use hardware devices and work with protocols, but they remain static and inflexible because they have few agility. These limitations make them difficult to manage and maintain day-to-day. To remedy this, SDN networks have been developed. On the other hand, the SDN networks are based on the centralization of the control plane. They use APIs to configure according to the needs; they are networks programmable at the time of the deployment and at a later stage according to the needs. They save in terms of flexibility, agility and virtualization.

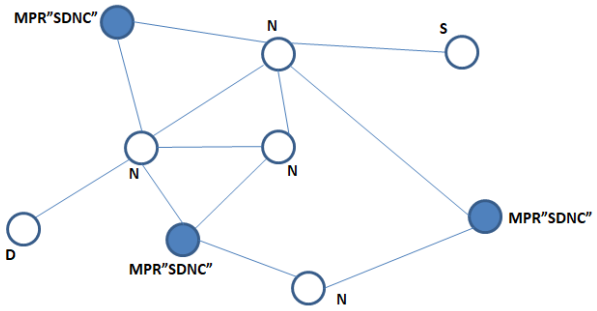

Fig. 4. Our proposed schema integrating MPR "SDNC".

Communication between the source (S) and the destination (D) is provided via proactive protocols. Besides the nodes (N), the presence of MPRs in our network makes it possible to optimize the transmission since it makes it possible to reduce sending control messages each time and optimizing the network. In our proposal, the SDN code will be integrated and implemented in the controller and we can therefore benefit from the security already integrated in SDN .In our case, the MPR will play the role of the controller, we will call them MPR"SDNC" (MPR SDN Controller) as shown in the figure above.

IV. Conclusion

In this article, we gave an overview of the MANETs networks and their architecture and infrastructure, and then we discussed the security of these networks by citing the security criteria and talking about the attacks that can harm these systems. We also presented the work already done in the security of the ad hoc networks and then we gave our proposal applying SDN security in MANETs.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

N. Mouchfiq conducted the research and all authors analyzed the data, wrote the paper and had approved the final version.

References

[1] D. Vukobratovic *et al.*, "CONDENSE: A reconfigurable knowledge acquisition architecture for future 5G IoT," *Internet of Things (IoT) in 5G Wireless Communications*, vol. 4, pp. 3360-3378, 2016.
[2] M. H. Shao, J. B. Lin, and Y. P. Lee, "Cluster-based cooperative back propagation network approach for intrusion detection in MANET," in *Proc. IEEE 10th International Conf. on Computer and Information Technology (CIT)*, July 2010, pp. 1627-1632.
[3] V. Srivastava and M. Motani, "Cross-layer design: A survey and the road ahead," in *Proc. IEEE Communications Magazine*, December 2005, pp. 112-119.
[4] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *EEE Wireless Communications*, vol. 11, no. 1, pp. 38-47, 2004.
[5] N. Goriya, I. J. Rajput, and M. Mehta, "Low control overhead for cluster maintenance in wireless network for DSR protocol," *COMPUSOFT*, vol. 4, no. 5, pp. 1736-1743, 2015.
[6] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoTFog networks from MitM attacks," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1156-1164, Oct. 2017.
[7] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "*SDN-based data transfer security for internet of things*," *IEEE Internet Things J.*, vol. 5, no 1, pp. 257-268, 2018.
[8] M. Xin, "A mixed encryption algorithm used in internet of things security transmission system," in *Proc. the 2015 International Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2015, pp. 62-65.
[9] T. T. Brooks, *Cyber-Assurance for the Internet of Things*. John Wiley Sons, 2017.
[10] IoT Challenges Advances Applications — Internet of Things — Telecommunication. [Online]. Available: https://fr.scribd.com/document/372075540/IoT-Challenges-Advances-Applications
[11] R. M. Ogunnaike and B. Lagesse, "Toward consumer-friendly security in smart environments," in *Proc. 2017 IEEE International Conf. on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, pp. 612-617.
[12] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 325-346, 2017.
[13] P. Krishnan, J. S Najeem, and K. Achuthan, "SDN framework for securing IoT networks," in *Proc. International Conf. on Ubiquitous Communications and Network Computing*, 2017, pp. 116-129.
[14] C. Benjbara, A. Habbani, F. El Mahdi, and B. Essaid, "Multi-path routing protocol in the smart digital environment," in *Proc. International Conf. on Smart Digital Environment*, Rabat, Morocco, July 2017, pp. 14-18.
[15] H. Amraoui, A. Habbani, A. Hajami, and B. Essaid, "Security-based mechanism for proactive routing schema using game theory model," *Mobile Information Systems*, vol. 2016, pp. 1-17, 2016.

Mouchfiq Nada was born in Casablanca, Morocco, in 1992. She received the state engineer degree from the National School of Electricity and Mechanics (ENSEM) attached to HASSAN II University, Casablanca, in 2016. She is currently pursuing the Ph.D degree with the Laboratory of Smart Systems (SSL), at the National School of Computer Science and Systems Analysis (ENSIAS) attached to Mohammed V University, Rabat, Morocco. Her research interests include the security of smart objects and systems based on new technologies.

Habbani Ahmed is a professor of higher education at the National School of Computer Science and Systems Analysis (ENSIAS) attached Mohammed V University, Rabat, Morocco and associate researcher at the laboratory in ENSIIE France. He received his Ph.D degree in applied sciences in laboratories of LEC (Laboratory of Electronics and Communications) of the EMI (Mohammedia School of Engineers) attached to the University Mohamed V Rabat, and LISIF (Laboratory of Instruments and Systems of Ile de France) of the Pierre et Marie Curie University, France. His research interests include modeling, development and implementation of mobile intelligent digital system, modeling, optimization, development and implementation of routing protocol (information collected to provide security, mobility, multipath and GPS rental), modeling, optimization, development and big data for routing protocol, modeling, optimization and Antennas, modeling, optimization, development, routing and smart grid, modeling, optimization, development and smart wireless sensors networks.

Benjbara Chaimae was born in Fes, Morocco, in 1989. She received the state engineer degree from the Sciences and Technologies Faculty attached to Sidi Mohammed Ben Abdellah University, Fes, in 2013. She is currently pursuing the Ph.D degree with the Laboratory of Smart Systems (SSL), at the National School of Computer Science and Systems Analysis. attached to Mohammed V University, Rabat, Morocco. Her research interests include improving routing in mobile networks.