International Journal of Wireless Networks and Communications.
ISSN 0975-6507 Volume 16, Number 1 (2024), pp. 1-13

http://www.irphouse.com

Assessment of the vulnerability to the Man in the middle attack of the ad hoc extension of the DOUNG (New Generation of Open Digital Universities)

Boukar Abatchia Nicolas, Mahamadou Issoufou Tiado, Maman Habibou Balkissa, Adamou Hassane Nassirou, Moctar Ousseini Madjiri

Department of Mathematics and Computer Science, Research team on Network and Telecommunication, University of Abdou Moumouni, BP 10662 Niamey – Niger

Abstract

The DOUNG (New Generation of Open Digital Universities), with a view to offering courses in synchronous mode adapted to learners, has extended its architecture, thus integrating Wi-Fi and ad hoc network technologies. As a result, learners can easily connect from their campus or in rooms and lecture halls with step-by-step propagation at a lower cost. This raises questions in terms of evaluation and optimization of parameters such as the security of exchanges and the quality of the services offered. In addition, the juxtaposition of open networks used in this architecture, combined with the implicit trust conferred on learners, further exposes the DOUNG to network attacks and particularly to the MITM (Man in the Middle) attack. In this paper, we propose to evaluate the vulnerability rate of the wireless extension of the DOUNG versus a MITM intrusion using the NS2 simulator with variable density and mobility, and routing ensured by the main protocols AODV, DSR, DSDV and OLRS and a stream transport of the SCTP protocol.

Keywords: Distance learning, DOUNG, Man in the Middle Attack, AODV, DSDV, OLSR, DSR, SCTP, ns2.

INTRODUCTION

The provision of distance education services has been disrupted in recent decades, moving from e-learning to open and more flexible models aimed at universal coverage. Thus, this approach will make it possible, on the one hand, to alleviate the problems of the demographic explosion, deleterious urban mobility and its security (road accidents)

and health risks (Covid19), and on the other hand, to adequately respond to the needs learners who were once satisfied with m-learning (mobile learning). As a result, learners' demands have become complex from a functional and technical point of view. As such, the DOUNG [1] offers a flexible model integrating the synchronous or asynchronous monitoring mode, the wired or wireless communication channel (with or without infrastructure), the mobile or desktop access terminal, and several tools to produce and use courses in the form of multimedia resources. This ubiquity advocated by this innovative model requires the support of technological developments such as Cloud Computing, high-speed internet, ad hoc network and VPN. This exponentially expands the attack surface, the perimeter to be secured and therefore subjects this model to new risks-oriented networks, systems and applications. In this paper, we will highlight the impact of the MTM (Man in the Middle) attack on the ad hoc extension of the DOUNG classroom by simulation under ns2. The indications on packet and energy loss as well as similar recent studies on QoS evaluation [2] [3] [4] we will serve as a criterion to compare the performance of the SCTP(Stream) transport protocol Control Transmission Protocol) with the main network protocols AODV(Ad hoc On-demand Distance Vector)[2], OLRS(Optimized Link State Routing)[3], DSDV(Destination Sequenced Distance-Vector) and DSR(Dynamic Source Routing)[4] in spaces similar to classrooms and lecture halls or to the learners' campus.

Architecture extended to the scale of a classroom

With the evolution of wireless and the emergence of mobile terminals (laptops, smartphones, etc.), learners can easily carry out multimedia activities. This possibility makes it possible to frequently find interconnected objects and high local wireless availability. It is with this in mind that the basic architecture of the DOUNG was extended in the research work [2] by deploying an ad hoc network from a Wi-Fi access point connected to the server of the backbone of this structure. This new proposed architecture [2] describes a four-part configuration. The first part consists of the NG-UNO server located on the backbone itself connected to the second part which is the WI-FI access point. The third part is the wireless network with infrastructure that accesses the WI-FI antenna for frontline learners. Finally, the last part is where learners distant from the antenna can follow the courses synchronously using the mechanisms of the ad hoc network. This wireless network constitutes the extension of the wired network hosting the server. From this extension, the problem of synchronous monitoring of DOUNG courses in this environment becomes an interesting perspective with the legacy of inherent and intrinsic threats to all these interconnected networks. The diagram of the extended architecture of the DOUNG is illustrated in Figure 1:

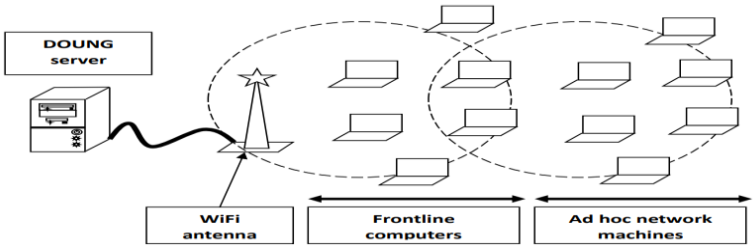


Figure 1: *Extension of the DOUNG architecture including an Ad hoc network*

Security challenges in the DOUNG network

Achieving global ubiquity of open universities requires the interconnection and interoperability of computer and telecommunications networks, whether wired, wireless, with or without infrastructure. This convergence of technologies used wisely by distance education exposes it to various security threats derived from vulnerabilities specific to these technologies and the velocity of threats. The notion of likelihood matrix, in risk management, is measured in terms of impacts on availability, integrity and confidentiality. It combines the probability of occurrence and the complexity of execution of a voluntary or involuntary event, likely to negatively impact an asset, however innocuous it may be [5], [6]. Even if the threat likelihood matrix is significant for network, system and application attacks [7] in the background of this work, we will focus on the main threat on the networks which represent the central point to achieve the objectives fundamentals of the DOUNG. In addition, cybersecurity is increasingly jeopardized with the evolution of artificial intelligence algorithms, quantum computing power and high-speed internet. Therefore, the rich and complex framework of the DOUNG constitutes an imminent target for cyber-attacks, particularly net

Work-oriented ones. The last major interest in network attacks lies in the fact that they constitute the entry point for other types of threats [8], [9]. Indeed, they are likely to exploit the flaws intrinsic to ad hoc networks (and wireless networks generally), and especially the implicit trust granted to learners; for other types of threats. This is of particular interest in intrusion attacks on networks with and without DOUNG infrastructure. The probability of occurrence of attacks is high given its recurrence and knowledge of past experiences on all communications channels [9] [10] devoid of security means used by the DOUNG. As a result, the juxtaposition of its networks in the hybrid learning model makes it even more vulnerable and subjects it more to a high frequency of successful attempts that can converge towards the highest level of occurrence of the first component of the likelihood matrix (value 4). The second parameter, or execution complexity of attack risk, is higher for wireless and infrastructure-less networks. Nevertheless, factors such as the crossing of the Internet, the accessibility of radio waves and the embryonic security of ad hoc networks, the popularization of the cloud, of IoT (Internet of Things) considerably make the implementation of these attacks at the lowest level of the matrix (level 1). We can deduct from the likelihood matrix of network attacks, especially those wireless and without infrastructure, a high risk for these types of threats. In addition, unlike companies which have perfect control of their assets and their users, universities have no control (or even no information) over the terminals of its learners. In addition, the intentions of learners also remain unknown and they can be infected to their output and serve as a Trojan horse. Thus, the scope of risks incurred by the information assets of the DOUNG, in particular the hosted services and even the learners, is expanding exponentially.

MITM attack on the DOUNG network

The MITM attack [9][10] aims to intercept communications between two peers (learner and learner or DOUNG), without either being able to suspect that the communication

channel between them has been compromised. Wireless channels with and/or without pre-existing infrastructure used to ensure a ubiquitous, low-cost and above all flexible learning model play favorably against MITM threats. As such, the ad hoc concept denying the paradigms at the heart of traditional network security plays a determining role to the detriment of the interconnection and interoperability of the networks it brings together. In addition, the intrinsic granting of the routing function to all nodes versus a restricted set of equipment (in a wired or wireless context with infrastructure) constitutes a notorious vulnerability. This facilitates the implementation of attacks on each node of these networks and increases the risks to the confidentiality and integrity of data and the availability of the services offered. The attacker is already in the position of router (in the middle of the nodes), he just needs to ensure that the right traffic passes through his channel by using his mobility and various techniques relating to the routing protocol family. After implementing the MITM attack, the attacker can decide to limit himself to listening and analyzing traffic, which constitutes a passive attack. In this case, it can be more aggressive and therefore more active, interfering in the administration, configuration and operation of the network. It would then risk injecting its traffic, modifying the operation of a node, usurping a valid identity, delaying, altering or deleting messages, causing a denial of services, overconsumption of energy, or network partitioning (selfish nodes). In our context, time being a primordial data for synchronous course monitoring, any disturbance which extends the delay or which causes the breakdown of synchronization between the teacher and the learner is likely to compromise the understanding of the message delivered. A lot of studies need to be done to determine the impact of the MIMT attack in the context of the DOUNG, specifically the administered portion of its network. Figure 2 below materializes the Man-in-the-Middle attack on the ad hoc extension of the DOUNG.

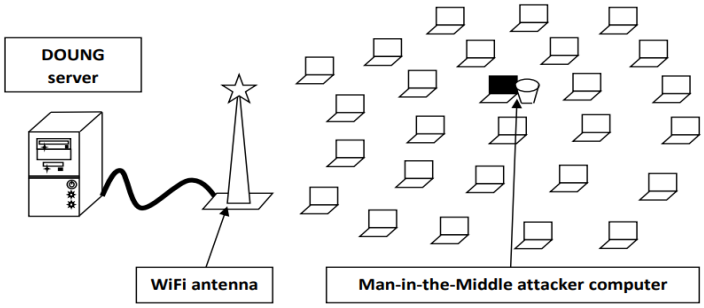


Figure 2: *Extension of the DOUNG architecture including an Ad hoc network*

The transport and network layer protocols used

The transport layer SCTP protocol

The activity of the SCTP protocol [RFC 4960] is based on two major principles, namely firstly, the response to events such as user calls, the arrival of segments or the management of timers. Second, the reaction of the SCTP protocol to each event depends on its current state. With these two principles, SCTP is referenced as bringing together

a set of event modules with change of state. Specifically, the operation of this protocol is based on the use of flows and association. An association is established before any transfer of information. It makes it possible to convey a set of flows without any order between them, in a form of grouping where the end points are known through a list of transport addresses, that is to say the combination of an IP address with a port number. By definition, a stream represents a sequence of messages with ordered transmission, which gives the SCTP protocol the position of a partially ordered, fully reliable transport layer protocol. SCTP is a reliable message-oriented protocol running on top of IP as a connectionless network layer protocol. The reliability of SCTP is also established through the transfer service with acknowledgment and without duplication, through the ordered data delivery service with an option of delivery by order of arrival of individual messages. Blocking one flow has no impact on the delivery of others. This protocol ensures tolerance to errors coming from the network layer through multiple domiciliation of nodes in different end points of the same association.

The AODV routing protocol

AODV [RFC 3561] is a reactive routing protocol using route discovery mechanisms and local connectivity maintenance. It quickly adapts to wireless network conditions while limiting overhead generation. Indeed, in its operation, it reduces the use of the network for its residual activities of determining available routes, which is expected to have a positive effect on the routing of real-time traffic. The creation of routing tables with the classic remote vector algorithm is based on the exchange of these tables between adjacent nodes. An initial table of a node first contains only the paths that link it to its immediate neighbors. With the diffusion in this neighborhood and the execution of the Bellman-Ford algorithm applied to each entry of a new table received, the updates lead to the progressive construction of the final tables containing all the destinations of the network. By implementing this algorithm, the AODV protocol of a node located on an active route broadcasts its routing table containing connectivity information using Hello messages and during a time interval fixed in milliseconds called HELLO_INTERVAL. Thus, the stability of the ad hoc network in the classroom allows the DOUNG to play on this parameter in order to extend the repetition times for the transmission of these messages. The expected effect is a significant reduction in ambient activity, generating significant overhead in the network. This reduction makes it possible to use the available bandwidth for the delivery of multimedia streams. When a sent Hello message is received by a neighboring node, the latter proceeds to create a new entry if it does not have any active route to reach the initiator of this message. Similarly, an AODV node may determine connectivity by listening to ambient activity or using route discovery. Route discovery initiated by the AODV protocol is related to its reactive nature. It is therefore only activated on demand, when the node waiting to send a packet placed in its sending buffer does not have a route to reach the specified destination. For this, the AODV protocol uses two types of messages consisting of the route request subject to a repetition frequency and the route response. However, the repetition frequency in the event of failure is limited, likewise, the interval between two consecutive route discovery attempts for the same target is doubled up to a threshold or exhaustion of the number of attempts or even up to receiving a valid route response.

The DSR routing protocol

The DSR protocol [RFC 4728] is a reactive protocol which performs routing by the source by allowing each node to reach its destination by propagation of the packet step by step. At the source node, the reception of data from the IP layer by the DSR protocol leads to the use of its own structures with invocation of appropriate mechanisms including the transmission of special messages. This could be the route discovery or route maintenance mechanism. Route discovery uses Route Request (RREQ) and Route Reply (RREP) messages. Route maintenance is done through transmission control (acknowledgments), route error management, packet recovery as well as segmentation allowing the size of packets to be adjusted to that of the paths taken. The operating scheme of the DSR protocol is based on the use by each node of the radio transmission power required to reach the next hop registered in the list contained in the packet. Regulation ensures power control to limit interference in the network. Thus, each node in the path caches the routing information taken from the packets it receives, including by extension by "sniffing" messages that are not intended for it. The packet traverses the network, being relayed by the nodes in the list to its destination. The unavailability of the path leads the source to transmit an RREQ packet propagated by broadcast with the nodes which are registered in the header list to the destination or to an intermediate node having the desired response using the cached information. An RREP packet is thus sent to follow the reverse path by this intermediate node constituting a free route response and containing the low energy consumption path. In the extreme case, the RREP is sent by the desired destination. A timer is managed to limit the frequency of repeating the route search for the same destination, knowing that the maximum number of attempts is also limited.

The DSDV routing protocol

The DSDV protocol [RFC 8965] is based on the Bellman-Ford algorithm. It introduces another routing philosophy with, for a node, the periodic broadcast of its routing table to its immediate neighbors during each significant change in the network topology. The node can use the "full-dump" update mechanism through which the DSDV sends its full routing table to all its immediate neighbors. The difference is that the node can use the "incremental" option which only allows routing table entries whose sequence numbers have changed to be transmitted. Another mechanism allows the use of timeout which forces the protocol to delay the transmission of its routing table entries to avoid early updates when better routes are discovered very early. All these mechanisms are of interest for our evaluation intended to highlight the adequacy of routing on the degree of vulnerability of the ad hoc extension of the DOUNG network to the MITM attack. This involves highlighting the mechanisms that facilitate the detection and correction of the consequences of this security threat during the synchronous monitoring of a course.

The OLSR routing protocol

OLSR has been proposed [RFC 3626] as a proactive routing protocol. It is designed to operate by reacting to the mobility of nodes in ad hoc networks, mainly in dense and poorly mobile networks such as the case of the ad hoc network in the DOUNG

classroom. It represents a form of link-state routing optimization producing routes consisting of the shortest path. The optimization of this routing is linked to the use of MPR (Multipoint Relay) multipoint relays instead for a node to communicate and broadcast to its entire immediate vicinity. The principle of multipoint relay is based on the rule which allows each node to choose a minimum subset of its symmetrical one-hop neighbors to reach the entire two-hop neighborhood. This chosen set of nodes called "multipoint relay" allows for optimized broadcasting by minimizing bandwidth usage and avoiding the periodic sending of control messages throughout the network. In classic flooding broadcast, a node retransmits any new message to its entire neighborhood. The optimization introduced by MPR adds a condition, retransmission only takes place if the message is recent and the node is considered MPR for the node from which it received the message. A non-MPR node N1 of node N2 does not retransmit the messages from N2 that it receives. From a functional point of view, the OLSR protocol of each mobile node carries out two operations bringing together the determination of neighbors by the periodic transmission of the Hello message (constitution of the MPRs) and the broadcast by each MPR of the TC message for the update of the network topology. A Hello message has multiple functions. It allows a node to populate its direct neighborhood table with link types. It also makes it possible to determine the nodes which have designated it as MPR (construction of the MPR-set list). An elected MPR node ensures control of the topology by periodically broadcasting to the members of its MPR-set, TC (Topology Control) messages allowing them to construct their topological table, then their routing table. OLSR uses the standard IP packet format to send control messages and provides hop count-optimal routes.

Performance evaluation by simulation

We considered a variable size and density (between 5 and 50 nodes/learners with a progression step of 5) similar to an average classroom or campus, with a Wi-Fi hotspot in accordance with the extended architecture of the DOUNG. This Wi-Fi terminal is the source of the courses given leading to the ad hoc network including a malicious node (MITM). The SCTP protocol is used for transport and DSDV, DSR, AODV and OLSR are implemented alternatively at the network layer. The IEEE 802.11 standard is used for the lower layers. The Wi-Fi access point is the source of CBR (Constant Bit Rate) traffic to the wireless local network containing the learners and the attacker. The classroom measuring 1500 x 300 is subdivided into two zones constituting the surface area of our simulation zone. The first 1/3 of the surface is used for the Wi-Fi antenna area and 2/3 for the ad hoc part. The position of the Wi-Fi antenna is fixed on the middle of the left side border. The attacker is included in the random distribution and nature of the mobility of the network nodes according to the principle of a “black hole” in order to systematically block all traffic passing through this node. The attack aims to cause a malfunction in the delivery and synchronous monitoring of courses through a drop in performance, blocking of traffic, induction of retransmissions and loss of energy and even partition of the network. By performing 150 seconds of simulation, the mobile nodes adopt the same moving speed between [0m/s, 10m/s]. We use the RWP (RandomWay Point) model according to the following 3 mobility styles: “mobility 0” where all nodes are inert and corresponding to maximum efficiency typically in a

classroom; “total mobility” or on the scale of a classroom which corresponds to a low mobility network like a campus; and finally “targeted mobility” inducing maximum connectivity by reorganizing nodes outside the attacker’s field of influence and mitigating or even possibly dissipating the impact of the attack. The latter moves all affected nodes to the healthy part of the network. The model of a river island is proposed in our context to refer to the direction of water propagation by analogy to the propagation of the media stream in the area of the attacking node. This model highlights the influence of the MITM attack in the ad hoc network of the classroom which blocks for certain nodes the progression of the multimedia stream emitted by the Wi-Fi antenna. For example, to better understand the impact of the attacker, the analogy is made by the river island model which is represents the effect of the MITM attacker on the multimedia stream emitted by the fragmented WiFi terminal in the form of packets from my Wi-Fi part to the ad hoc zone. This topology is illustrated in Figure 3:

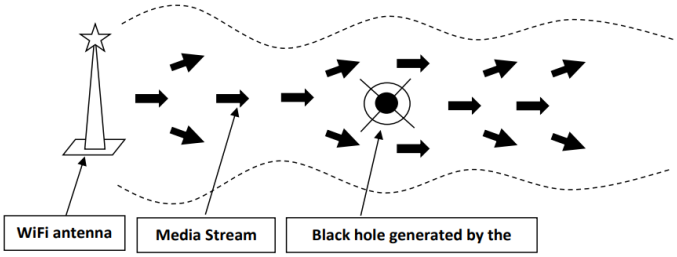
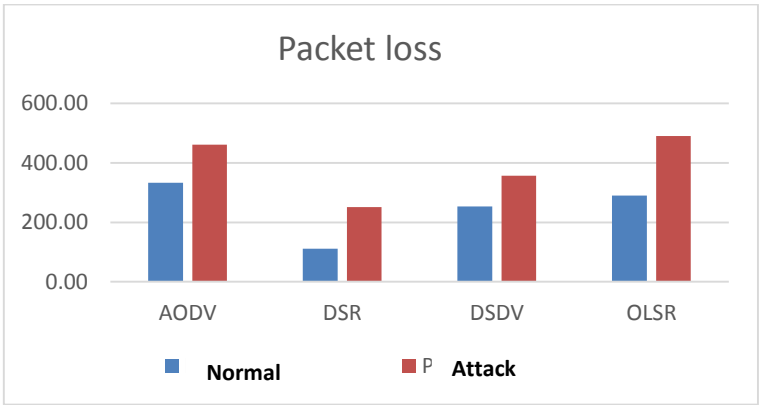


Figure 3 : *Model of a river island or black hole for the Man-in-the-Middle attack*

Results interpretation

We carried out this experiment with the aim of determining the best routing protocol that is perfectly suited to the wireless extension of the DOUNG network, whether it is a confined space (room or amphitheater) or free (mobility on campus). The second part of our work consists of evaluating the vulnerability of this extension to the MITM attack. And from the latter, arises a search for a solution to overcome the aspects of confidentiality and the integrity of exchanges and the availability of services that may result following a MITM intrusion into the interactions of the resulting learning public.

Overall impact of the attack



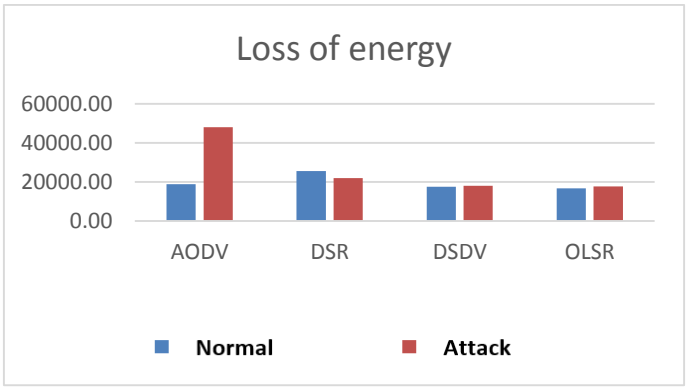


Figure 4*: Overall summary of results*

The MIMT attack resulted in over 60% packet loss regardless of routing protocol, mobility and density. In energy terms, we notice a 70% increase in residual energy. These two indicators are explained respectively by the absorption of traffic by the MIMT node on the median positions generating isolation from the network nodes and by the selfishness of the latter. This demonstrates in more than one way the degree of nuisance of this attack. To best interpret these results, we will focus on mobility styles and routing protocol characteristics in the following sections.

Impacts of the attack according to learner mobility

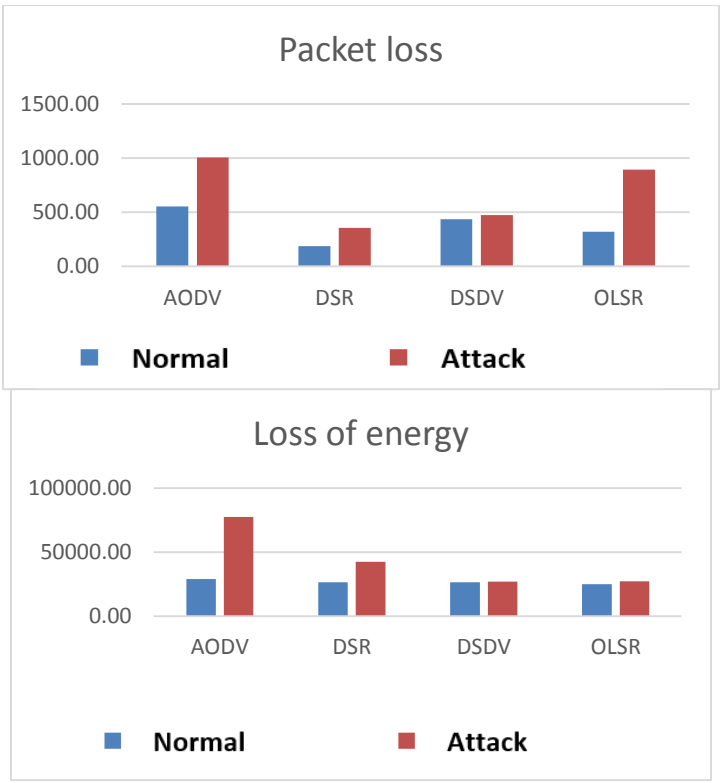
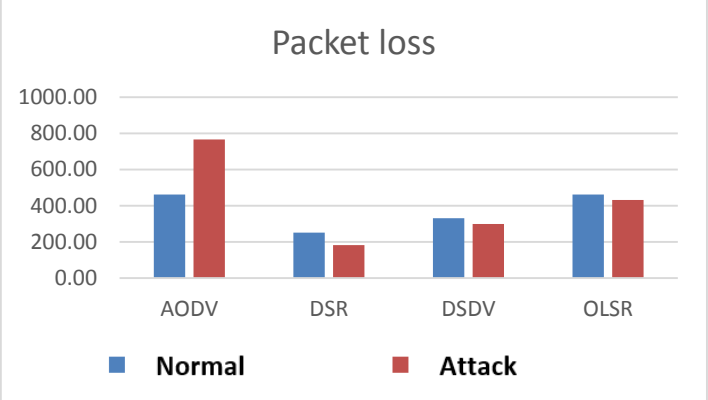


Figure 5 : *Consequences of learner mobility and the MITM attacker*

In the stationary scenario, the packet loss (difference between received and transmitted packets) is higher of the reactive AODV protocol due to its slowness in updating the paths (even if the packets do not reach the destination). The DSDV protocol generates less packet loss through its shortest path search mechanism in front of AODV. As for the DSR and OLSR protocols, they offer good mitigation of the effect of the attack with clear effectiveness in favor of the DSR. This is explained by the absence of residual activities and the effectiveness of its source routing principle combined with its basic route discovery and maintenance mechanisms. Unlike, OLSR still maintains its residual bandwidth-consuming activities through the organization of the network and the search for the shortest path for route selection. When the network is mobile, we also see a higher loss rate of the AODV protocol than that of DSDV. This shows the difference in the influence of mobility and attack on these two protocols. Indeed, paths are created and destroyed with mobility and residual activities are repeatedly restarted. As a result, packets in intermediate buffers may get lost in transmission. To illustrate the difference in their operation, the AODV protocol focuses on the distance to carry out routing and builds the path on demand each time. As for the proactive DSDV protocol, it also relies on distance for routing but periodically broadcasts a control message to create, maintain and update routes. The DSR reactive protocol also remains the least vulnerable to the MITM attack in this scenario. On the other hand, the proactive OLSR protocol remains the most handicapped with difficulties in selecting routes induced by the repetitive reorganization of the overall vision of the network in order to route packets. The isolation and selfishness of the nodes promotes a clear improvement in autonomy (energy difference between the start and end of the simulations) regardless of the routing protocol.

Impacts of the attack and the corrective solution



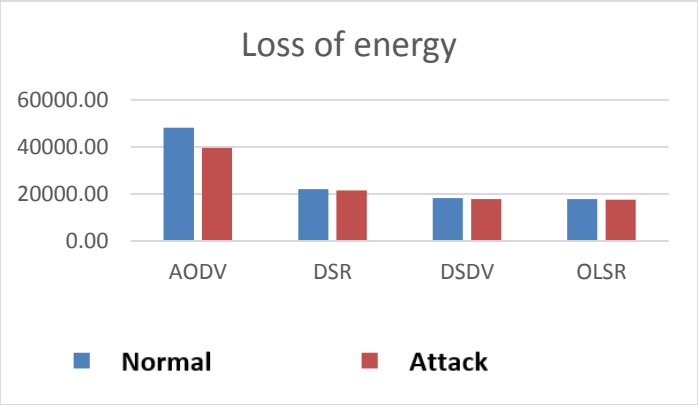


Figure 6: *Search for a palliative solution based on the geographical position of the attacker*

Targeted mobility, consisting of geographically isolating the MITM attacker, maintains the order previously obtained according to packet loss. Indeed, AODV is the most vulnerable to packet losses, while DSR is the most resilient. Even if network mobility works to the detriment of OLSR and DSDV, the restriction of space caused by palliative mobility largely favors DSDV. Thus, putting the nodes in the infected zone out of the reach of the MITM attacker causes a reduction in performance relating to transmissions in certain cases. However, with the exception of SCTP/AODV, the SCTP/OLRS, SCTP/DSDV and SCTP/DSR stacks react favorably to the trapezoid model with a gain varying between 12% and 14%. In terms of energy, we see a slight drop in the temporary and spontaneous mobilization of nodes to isolate the attacker. This is explained by the artificial reorganization of the network and the negligible partitioning delay of infected nodes. This style of mobility is promoter and therefore guides our perspectives for designing intrusion management and optimization models based on communication between the transport and network layers used within the framework of DOUNG.

CONCLUSION

In this paper, the MITM intrusion was evaluated on the ad hoc extension of the DOUNG network who constitutes its Achilles heel. Thus, the SCTP/AODV, SCTP/OLSR, SCTP/DSDV and SCTP/DSR protocol stacks were used to highlight the consequences of this attack on peer-to-peer sharing between learners involved. Since energy is not a determining factor in university areas and given its relative stability, it is undeniable that the SCTP/DSR stack is the most resilient to the MITM attack regardless of the density and mobility of the nodes and the palliative solution based on the geographical position of the attacker. In short, the contribution of the present work, in addition to directing towards solutions for managing MIMT intrusions in ad hoc networks, concerns the mobility of the nodes which unequivocally determined DSR as the appropriate routing protocol to deploy on the campuses, classrooms and lecture halls of open universities. This confirms the position of SCTP/DSR as the suitable stack for the extended DOUNG architecture in terms of QoS (Quality of Service) highlighted in

recent studies [2][3][4] and resilience to the MITM attack and its underlying threats. Future research perspectives will consist, among other things, of finding a correlation between the metrics of the evaluation of the quality of service and of being able to improve the performances and the responses to the MITM attack by using the algorithms of the artificial intelligence (machine learning) and the Cross Layer mechanism.

REFERENCES

[1] M. I. Tiado & H. Saliah-Hassane, "Cloud-Computing based architecture for the advent of a New Generation of Digital OpenUniversities in m-learning", ICEER 2013 conference, Marrakesh –Morocco, July 2013, ICEER13 Proceedings, pp572-579, ISBN 978-9954-9091-2-6.

[2] I. G. Noura, M. I. Tiado, H. G. Souleymane, C. D. I. Hussein, H. M. Mahamadou, "Quality of Service evaluation by using Ad hoc on Demand Distant Vector (AODV) in the classroom ad hoc network of the New Generation of Digital Open Universities (NG-DOU)", Advances in Wireless and Mobile Communications (AWMC), ISSN 0973-6972 Volume 13, Number 1 (2020), pp. 11-22, © Research India Publications, http://www.ripublication.com

[3] I. G. Noura, M. I. Tiado, H. G. Souleymane, C. D. I. Hussein, H. M. Mahamadou, "Quality of Service evaluation by using Optimized Link State Routing (OLSR) in the classroom ad hoc network of the New Generation of Digital Open Universities (DOUNG)", Advances in Wireless and Mobile Communications (AWMC), ISSN 0973-6972 Volume 13, Number 1 (2020), pp. 23-33 © Research India Publications http://www.ripublication.com

[4] M. I. Tiado, I. G. Noura, H. G. Souleymane, C. D. I. Hussein, H. M. Mahamadou, "Searching a Quality of Service (QoS) routing protocol adapted to the ad hoc classroom network of the New Generation of Digital Open Universities (DOUNG)", International Journal of Wireless Networks and Communications (IJWNC). ISSN 0975-6507 Volume 1 2, Number 1 (2020), pp. 1-11 © International Research Publication House, http://www.irphouse.com

[5] Ning Zhao;Xudong Zhao;Meng Chen;Guangdeng Zong;Huiyan Zhang, "Resilient Distributed Event-Triggered Platooning Control of Connected Vehicles Under Denial-of-Service Attacks", IEEE Transactions on Intelligent Transportation Systems (2023), Page(s): 1 - 12, ISSN: 1558-0016, DOI: 10.1109/TITS.2023.3250402

[6] Brent Pethers, Abubakar Bello, "Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks", Future Internet 2023, 15(1), 29; https://doi.org/10.3390/fi15010029

[7] Maikel Lázaro Pérez Gort, Martina Olliaro, Agostino Cortesi,"Relational data watermarking resilience to brute force attacks in untrusted environments", Expert Systems with Applications, Volume 212 (2023), https://doi.org/10.1016/j.eswa.2022.118713

[8] Mazin Abed Mohammed, Abdullah Lakhan, Dilovan Asaad Zebari, Karrar

Hameed Abdulkareem, Jan Nedoma, Radek Martinek, Usman Tariq, Majed Alhaisoni, Prayag Tiwari,"Adaptive secure malware efficient machine learning algorithm for healthcare data", https://doi.org/10.1049/cit2.12200 (2023)

[9] Saketh Kumar Kanisetty; Nagalakshmi Jayalakshmi Thiruchitrambalam, "Design of intrusion detection system for wireless adhoc network in the detection of man in the middle attack using support vector machine classifier method comparing with ANN classifier", AIP Conference Proceedings 2655, 020111 (2023), https://doi.org/10.1063/5.0119113

[10] Constantinos Louca, Adamantini Peratikou, Stavros Stavrou, "A novel Evil Twin MiTM attack through 802.11v protocol exploitation", Volume 130, July 2023, 103261 Computers & Security