International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 12 (2020) pp. 193-203

Received: 21 Jan, 2020; Accepted: 9 May, 2020; Published: 6 June, 2020

Uncertainty-based Data Collection in Mobile Ad-Hoc Networks

Rahma MEDDEB[1], Bayrem TRIKI[1], Farah JEMILI[1] and Ouajdi KORBAA[1]

[1]Universite de Sousse, ISITCom, MARS Research Laboratory, LR17ES05, 4011, Hammam Sousse, Tunisia.
rahma.elmeddeb@mars.rnu.tn, bayrem.triki@gmail.com,
jmili_farah@yahoo.fr and ouajdi.korbaa@mars.rnu.tn

Abstract: **As an important security measures in Intrusion Detection System (IDS), Data Collection process monitors data in the network and supports network performance evaluation. Therefore, Data Collection plays an essential and a crucial role in distributed IDSs. Accordingly, the key idea of our proposed approach is to implement an effective and an adaptive data collection mechanism that could enhance the efficiency of the detection and identification of malicious nodes. In addition, we propose an efficient in-depth collection and analysis of data in mobile networks for intrusion detection system based on a uniform set of evaluation criteria. We note that the uncertainty present in the data collected represents a major challenge. Our proposed solution enhances intrusion detection efficiency by tacking into consideration incomplete information about occurring malicious nodes. This paper focuses on Denial of Service (DoS) attack scenarios within labeled datasets and specially the detection of the most potential threats that can disrupt the availability of routing services in mobile Ad-Hoc Network.**

Keywords: Mobile Ad-Hoc network, Intrusion Detection System, Trustworthy Data collection, Measurement Uncertainties, Labeled dataset, Machine Learning Algorithm.

I. Introduction

Nowadays, wireless communications are omnipresent. They are witnessing a dizzying growth all around the world. Wireless communication has a crucial role to play within Data Communication Networks, which may offer viable solutions to provide the mobility of mobile nodes as well as essential services wherein the installation does not rely on infrastructure [1]. Mobile Ad-Hoc networks (MANETs) have obtained much attention thanks to their flexibility and scalability. However, when we enjoy the benefits and conveniences brought in MANETs, we find that they appear to be more susceptible to various attacks and intrusions [2]. Hence, Mobile networks will require more security or more safety scheme to ensure its communications [3]. Due to their nature MANET (large-scale, self-organization, dynamic topology, and constrained resources), the mobile network makes some information unavailable and/or incomplete required for the intrusions detection process. Intrusion Detection Systems (IDS) is a process that controls the behaviors and activities in order to detect illegal and abnormal activities [4]. Network-based Intrusion Detection System (NBIDS) is the several efficient ways to defend against malicious nodes in Mobile Ad-hoc Networks [5]. In order to detect malicious activity, the Intrusion Detection System typically consists of two types of components: Data Collection (DC) and Data Analysis components (DA). The first component executes data monitoring from the network and supports network performance evaluation. Therefore, DC plays an essential and crucial role in distributing IDSs. The second component incorporates the DA method that analyzes the data collection to detect malicious activities. Many solutions have been given to ensure the security of mobile networks providing a review of security data collection and mechanisms of data analytics for detecting attack. Some recent surveys focus on data collection mechanisms and data analytics in the MANETs. The authors in [6] studied various prominent IDSs in MANETs, which are with related technology and detection process. In this article [7], the authors exhibit network security-related data, including its characteristics, and the applications of data collection. Its provide the objectives and requirements of data collection and give a taxonomy of security-related data collection technologies. In this paper [8], the authors present the related research in terms of network data for security detection, data compression and fusion for economic data storage and efficient intrusion detection. A comparative analysis of present techniques for future directions in purpose and implementation of intrusion detection systems. It is noticed that there is no globally trusted metric for evaluating the efficiency of current and upcoming detection systems. Regarding network data collection for security measurement, many studies of network traffic analysis solutions were published in [9], [11]. These reviews focus only on data collection mechanism in a mobile network. The literature, we have considered, can rarely compare the performance of data collection mechanisms. Based on their proper experimental parameters that do not correspond with other papers and do not allow different studies to be comparable. Therefore, that to collect and analyze data collection efficiently, researchers proposed a lot of architectures and solutions. However, none of them did consider the process of collecting and measuring

data on features of interest in analyzing data. For specific mobile network scenarios and specific mechanism of data collection purposes, the requirements of network data collection are different. Therefore, in the process of data collection, it is not required to analyze all data traces extracted from the networks. The nodes data collectors are required to collect useful data information, meaningless and useless data information should be discarded. In addition, redundant information from data collection should be eliminated to be analyzed by the data analysis component [5]. This article is divided into six sections. The section II shows the motivating Mobile Ad-Hoc Network deployment and a literature review of existing Intrusion Detection Techniques for MANETs. Section III, it discusses the main issues related to intrusion detection and the routing availability challenges in MANETs. Section IV presents the Trustworthy of security-related data collection in mobile networks for the purpose of detecting mobile intrusions and measuring security for Ad Hoc networks. Section V introduces the suggested architecture and highlights our contribution to data collection and analysis method. The simulation results are given in Section VI, which demonstrates that the proposed approach is adequate in terms of network defense and intrusion detection in Mobile Ad-Hoc Network. The closure of this article shows our conclusions and mentions the implications for practice and recommendations for future research.

II. Background Intrusion Detection in MANET

A. Intrusion Detection Techniques for MANETs

In order to detect a malicious activity, the Intrusion Detection System typically consists of two types of techniques: Data Collection Technique and Data Analysis Technique (see Figure 1).

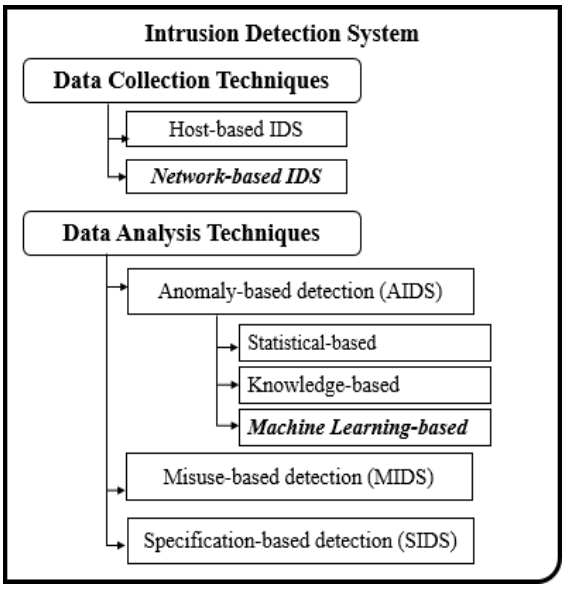

Figure. 1: Intrusion Detection Techniques for MANETs

According to Data Collection Techniques, intrusion detection can be categorized based on audit data as either Host-based or Network-based. Network-based IDS works on a specific node and collected audit data from the mobile network traffic that flows through it, and then examines the data collected. While Host-based IDS acquires this data through hope rating of system log files that run on the mobile node. Based on Data Analysis Techniques, IDSs can be classified into three categories as follows [10]:
Anomaly-based detection (ABIDS), Misuse-based detection or Signature-based detection (MBIDS), and Specification-based detection (SBIDS). In ABIDS technique, the normal behavior of the target system (network and mobile nodes) is explained, and a profile or a normal behavior model is constructed according to it. Based on this profile, a threshold is determined, which shows the boundary of usual and unusual behaviors. Then, the network and the nodes are controlled and if any behavior unmatched with the normal behavior is observed, it is considered as a malicious node. In MBIDS, known patterns of intruders are kept. Then the behavior of the mobile network and its nodes is measured. When any unusual behavior is observed, it is compared with the existing patterns. If a behavior matches with existing patterns, it is considered as a malicious node. In SIDS, system defines a set of constraints that define the correct operation of protocol or programs. Then, it observes the execution of the protocol or program with respect to the prescribed constraints. If the behavior of a node or network is deviated from these constraints, it is reported as a malicious node. Obviously, the first phase in detecting attacks and intrusions is to collect security-related data. However, in IDS based on Network-based, there exists a number of challenges in data collection. Briefly, we first provide the requirements for data collection and present a review of data collection technologies in MANETs. Besides, we analyze the existing collection nodes and collection mechanisms in terms of network data collection and analyze them based on the proposed requirements and objectives towards high-quality security-related data collection. This research focuses on Data Analysis detection techniques, based on soft computing techniques and machine learning. This technique has independently the potential to analyze the collected data from network traffic. The ability of supervised Machine Learning algorithms that handle these datasets can use patterns that were observed in previous data to make decisions for the new evolving data patterns in the network traffic. These supervised algorithms based Intrusion Detection Systems which very effective to defend against a wider range of security threats [5]. The next section provides a comprehensive study of most prominent security-related data collection in intrusion detection for the purpose of trustworthy security measurement. Besides, an attempt has been conducted to compare several intrusion detection techniques with their operational strengths and limitations.

B. An overview of Data Collection and Data Analysis Techniques

In order to measure and evaluate the security of MANET and make this mobile network react accordingly, a more promising alternative is to represent IDS that plays the role of outside defense system to detect intrusions in Mobile Ad-Hoc Networks. A large variety of intrusion detection systems has been proposed for wired networks [12]. Nevertheless, their implementation in MANETs makes it ineffective and inefficient for this open environment due to its specific features. Accordingly, it motivates researchers to the development of most specific solutions for intrusion

detection in MANETs. We notice that in most intrusion detection mechanisms, it is crucial and necessary to collect security-related data for further analysis. We propose to represent the most comprehensive study on existing data collection architectures, methods and mechanisms in the literature.

Based on Markov chain classifier, the proposed an Anomaly-based IDS [13]. In the route discovery phase of Dynamic source routing protocol (DSR), a node collects two features as the input of the intrusion detection system, where every mobile node maintains these features in their routing table. First one is the percentage change in the route (PCR) and the second one is the percentage change in the number of hops (PCH). In this proposal, multiple detection engines are situated on every mobile node. The local detection engine collects and processes the routing information to detect disruption attack in MANETs. In the next proposal [14], they further extended the study on intrusion detection in MANET using a Markov chain classifier in which mobility of the nodes is considered as the principal feature for evaluating the performance of the network. The data collection module of each IDS agent measures the LCR over records auteurs by periodically collecting the local link data. The Euclidean distance value between LCR and current LCR is utilized to identify the anomaly.

Strength: The detection scheme in [13] reduces the meantime to the first alarm, also improves the detection accuracy by the deployment of multiple detection engines at each mobile node as well as the correlation of data collection and alerts from the neighboring mobile nodes. The intrusion detection method in [14] is very efficient in the case of nodes mobility.

Limitation: The detection method in [13] also enhances the processing and communication overhead as multiple detection engines installed on every mobile node have to regularly exchange detection reports and alerts with neighboring nodes. The detection scheme in [14] is rendered ineffectual and difficult with the static training process.

In [15], Li et al. presented an intrusion detection scheme using Support Vector Machine and integral fuzzy network (SVMFN) to detect routing attacks. SVMFN integrates multiple classifiers so that classification at a low bit rate occurs efficiently.

Strength: This scheme [15] detects the routing attacks with high detection accuracy. It is achieved using SVMs based intrusion detection techniques. Furthermore, the feature selection for SVM algorithm also affects the flexibility of the IDS for high dynamic environments.

Limitation: The approach [15] is not suitable for a large scale network. It requires a separate mobile network for each kind of attack; otherwise, it suffers from the high-false positive rate.

The proposed approach in [16] is defined to detect the selective Blackhole attacks in MANETs by using an anti-Blackhole mechanism (ABM) in all the nodes in the network. All IDS nodes are deposited in a promiscuous mode to sniff the routing packets, by which the suspicious value of a mobile node can be estimated by the difference between RREQs and RREPs messages. If any mobile node does not broadcast a RREQ and forward a RREP for a specific route, then the suspicious value of the node will be increased by one in suspicious node tables of neighbors IDSs nodes.

Strength: in this scheme [16], the exchange of information about malicious node between the neighboring nodes obtain better efficacy for the prevention of Blackhole attack.

Limitation: the anti-Blackhole mechanism [16] is supposed that a node ID cannot be forged, and a message sent by an IDS node cannot be modified. All IDS nodes are ordered to be deposited in sniffing mode that results in more power consumption.

An ABIDS for detecting the Denial of Services attacks have been proposed by the author supposes the presence of a Central Entity (CE), which consists of two phases: training and testing phase [17]. Phase one is supposed to be free of malicious nodes and reflecting the normal behavior of a mobile network. Thereafter, during the second phase, the CE node collects the information from all the mobiles nodes, determines the probability distribution, and then compares it with the normal behavior profile using the chi-square Independence test for identifying any difference from normal profile. Consequently, the Central Entity notifies all mobile nodes to blacklist the detected malicious behavior/(s).

Strength: This technique [17] reduces false-positive rates.

Limitation: This approach [17] relies on Central Entity to detect anomalies nodes, which is a challenging task due to distributed nature and stringent resources of Mobile networks. It acquires high computational overhead over CE node because of the collecting and processing of large data collection. The Central Entity may be a single node of failure.

Intrusion detection and adaptive response mechanism (IDAR) is presented by [18] that applies a combination of Misuse-based techniques and statistical Anomaly-based to improve detection accuracy. IDAR Hybrid proposed to provide a flexible response to attacks instead of a static response without isolating the affected node. It is an example of using IDS solving MANET attack vectors. In the proposal all nodes work in one of the three manager nodes (MN), cluster heads (CHs) and cluster nodes (CNs). Two matrices are utilized to collect the routing-related information: network characteristic matrix (NCM) and performance matrix (PM). In the data collection phase, the CHs collect the information from their CNs after each time interval (TI) and derive the matrices. Then, CHs report these matrices to MN.

Strength: IDAR [18] uses a hybrid approach both Misuse-based and Anomaly-based techniques, responds to intrusions in a flexible adaptive method. In other words, it selects a response on the basis of the confidence level of detected intrusions and malicious nodes severity and network performance degradation.

Limitation: IDAR mechanism [18] relies on manager nodes to detect anomalies, which may be a single point of failure, and this approach suffers from large data collection and processing overhead as network view is updated after each time interval.

Hybrid intrusion detection is presented by [19], where Conformal Predictor K-Nearest Neighbors algorithm (CP-KNN) is applied as Anomaly detection and Distance-based Detection (DOD) algorithm is applied as Misuse detection. The Data Collection module collects audits data from various network sources and passes it to Pre-process Module. This module selects an informative feature from all features set, and then transfers these features to the Local Detection Module. This module examines the collected data using CP-KNN and DOD algorithms and identifies attacks in the MANETs. In this approach, the detection module consists of

two main components: local intrusion detection (LID) and gateway intrusion detection (GID). The first one runs at each mobile node and performs local data collection. If a malicious node is detected with weak evidence, then it initiates the signals to the nearest gateway node (GID) to trigger an intrusion detection procedure.

Strength: The hybrid detection approach (Anomaly detection and Misuse detection) [19] increases detection accuracy.

Limitation: The more traffic data exchanged over the mobile network can hamper the Ad-Hoc mobile network performance [19].

Based on the state transition analysis [20], an Intrusion Detection System called AODVSTAT is proposed using a state transition analysis technique (STAT) for detecting the malicious nodes (packet dropping and spoofing attack) against the AODV routing protocol in MANETs. In this mechanism, events are either data packets or AODV control packets. The detector nodes (i.e., an observer) monitor the behavior of neighboring nodes by overhearing the traffic. If any neighboring node does not forward the routing messages within a certain time interval, it indicates that the mobile node is behaving as an intruder. AODVSTAT node has two modes of operations: standalone mode witch, the sensor detects the malicious node within its neighborhood nodes only and distributed mode witch, the sensor exchanges the updated messages of each node.

Strength: AODVSTAT [20] detects various types of attacks accurately. State transition analysis can help to maintain known attacks for instance as a series of states. By employing the STAT, an intrusion can be represented as the sequence of the state changes from a secure state to a compromised state.

Limitation: this mechanism [20] does not set how to update the attacks signatures at all detectors node. It is not addressed in this step.

In [21], the authors designated a specification synthesis to design and analyze routing protocols in Mobile Ad-Hoc Networks and to define how the protocol evolves from one to another configuration. Such a specification model will explicitly include all possible monitored behavior of this protocol. Moreover, this proposed approach generalizes the specification with an attempt to include additional behavior of the protocol that is not known to be abnormal. Based on the specification of protocols that can be extracted from network traffic flows and expressed as directed graphs where mobiles nodes represent the routing protocol configuration and directed-edges between nodes. Therefore, they employ this specification to detect malicious behavior, and have validated and constructed specification protocol.

Strength: In the specification model [21], the network behavior and required feature set is directly obtained from the specification of the routing protocol that enhances the accuracy of attack detection. The scheme is also able to detect unknown malicious nodes.

Limitation: This scheme [21] cannot detect the source of the intruder of malicious behavior.

In this proposed [22], the author designed a specification-based IDS model called SIDM by using a method called Previous Two Forwarders (PTF). The PTF method can ensure the integrity of routing packets. It can provide the correctness of collected data (mutual and non-mutual data), where the first one represents Hop Counts (HC) and the second means other features such as Sequence Number (SN), RREQ packet, and IP address. This mechanism enforces the exchange of packets to comply with the specification of the routing protocol. In this case, the detection rules are specified with the AODV protocol. The intermediate nodes transmit the packets with supplementary information concerning PTF nodes. The receiver node compares the previous messages with the received to ensure integrity. A Central Authority (CA) authenticates all the nodes before they join the mobile network, and a digital signature is used to protect the packets from being tampered.

Strength: In this proposed [22], the external attacks cannot join the mobile network as a CA authenticates all the mobile nodes and integrity of messages are maintained by digital signature.

Limitation: This method [22] is difficult and inadequate to be considered for Mobile Ad-Hoc Networks environment, as CA is required to schedule the authentication process. This method increases the processing and communication over-head over the mobile network.

In [23], the authors explore application-layer tunnels detection such as DNS, HTTP and HTTPS tunnel and introduce a generic detection method by using both Domain Generation Algorithm (DGA) filtering rules and machine learning algorithm. The detection method mainly consists of five modules: (1) Data collection module is responsible for collecting communication data; (2) Rule-based DGA filtering module is defined to extracts the domain name and then matches them with the proposed filtering rule; (3) Data preprocessing module is responsible for performing feature extraction and feature construction for communication data; (4) Machine learning module is used to classify the communication data to detect whether there is a tunnel; (5) Network connection blocking module can block data transmission and cut off the network connection.

Strength: [23], this method can improve the efficiency and real-time performance of application-layer tunnel detection.

Limitation: [23], the authors do not examine protocol payload data but only consider the protocol header and communication behaviors. This scheme detects application-layer tunnels attacks only.

The authors in [24] present the study and implementation of an adaptive security-related data collector in heterogeneous networks. The collector solves the issue of heterogeneity of the network by creating a Security-related Data Description Language to instruct security-related data collection in many networks. It applies adaptive algorithms to reduce the collected data.

Strength: in [24], by introducing two adaptive sampling algorithms to security-related data collection to improve collection ability, assure collection accuracy and reduce the quantity of the data collection to minimize the effect of data on the operations of the network.

Limitation: This approach [24] only evaluates in the contexts of the Internet and LTE.

We review some existing Intrusion Detection Systems and then exercise representative IDSs for comparing and evaluating involved security-related data collection methods.

Table 1 provides a summary of some of the MANET Intrusion Detection System mechanisms studied in this section, where sufficient knowledge is available in the referenced papers, using these features as Table 1. We can

see from Table 1 that the IDS mechanisms generally use either Anomaly-based IDS (ABIDS), Misuse-based IDS (MBIDS) (i.e., or Signature-based IDS) or Specification-based IDS (SBIDS) techniques to identify intrusions in mobile networks, but hybrid techniques, have been developed in some cases to deal with network layer attacks [18], [19]. In addition, we observe that there are mechanisms that deal with multiple attacks by implementing Markov chain classifiers [13], [14] and another method Inductive Logic Programming (ILP) [18]. The completed comparison and evaluation shown in the above tables identify several open issues on security-related data collection in mobile networks. We furthermore notice (Collected Data Type column) that most of the proposals do not consider a generic method for data collection. Through a detailed analysis, we suggest an adequate approach about security-related data collection.

According to several proposed evaluation criteria, we evaluate the performance of these data collection mechanisms and summarize their main characteristics. Table (see Table 1) provides a summary of some of the MANET Intrusion Detection System mechanisms studied in this section, where sufficient knowledge is available in the referenced papers, using these features as Table 1.

II. Trustworthy Data Collection Technique

In this section, we study the reliability of security-related data collection in mobile networks for the purpose of detecting mobile intrusions and measuring security for Ad Hoc networks. First, we specify a number of requirements in terms of collecting reliable security-related data. Then, we determine the issues related to data collection and evaluation metrics from a database that should be collected from IDS nodes for the detection of various attacks in mobile networks.

A. The data collection requirements

Intrusion detection systems process the relevant data to detect intruders. If the data collected is not sufficient to ensure the accuracy of the detection, the detection analysis gives an incorrect result. Thus, the reliability requirements of the data collected are essential. Therefore, care must be taken to ensure that the data collected which were by the node IDS does reflect the behavior of the mobile node. Consequently, some requirements can be obtained as follows.

1) Data Reliability

The accuracy of intrusion detection and security measures is greatly dependent on the reliability of the data in the dataset. Mobile nodes may offer incorrect data due to the influence of the environment on its operation. Therefore, we had chosen, that mobile nodes can be classified into two classes: Normal nodes and observer nodes (IDS nodes). It should be emphasized that these observer nodes or data collectors can be reliable sources to provide the data collection phases and contribute to a reliable and precise database.

2) Data stability

Stable data collection refers to the ability that observer nodes can reach data from mobile networks. There are a few reasons why a data collector fails to collect data, such as network congestion and the sender's selfishness. Provided that enough data cannot reach the data collector, a calculation detection result is not reliable, which has a negative impact on the measurement of the security of MANETs. So, in order to be able to collect enough data to improve the accuracy of attack detection. What we are proposing is to provide some stability with observer nodes in order to guarantee the high accuracy of detection by allowing data generated which were to reach as much observer node as possible.

3) Data synchronization

It is necessary to have a synchronization to analyze the behaviors of a mobile node deviating from its habits. Synchronization requires that all affected data collectors aggregate simultaneously the data collected for attack detection efficiency. If this property cannot be reached, a variant of an attack could lead to different sequences of events, rendering detection ineffective. Data synchronization mechanisms should be studied in more detail in order to obtain an accurate measure of security. However, it is difficult to achieve absolute synchronization in MANETs.

We need to measure the clock offset between the different observer nodes and calculate the time adjustment function to synchronize them. Depending on the results of the estimation, the data collectors can select the data that satisfy a certain specific degree of synchronization. However, if a data collector chooses data with the high degree of synchronization for data collection, there may be little selected data, which decreases the accuracy of detection due to insufficient data for detection.

B. The challenges of data collection

If we abstract from the technical issues related to the generation of behavioral databases from collected data (taking into account the mobility of nodes, etc.), many issues remain concerning by the exploitation of the information mentioned in the collected behavior set. Indeed, the simulation of behavior of the nodes was defined, in the first place, in normal profiles of a mobile node in MANET. The malicious nodes were then programmed to run them, thereby simulating mobile network activity. The attack scenarios were designed and executed to express cases of malicious behavior in the network. These collected behaviors belonging to the evaluation of the information can be represented by the evaluation of the sources of the data and the analysis of behavior, one approaches to certain in-depth analyzes such as imprecision, uncertainty, redundancy, etc. The analysis carried out was multifaceted; the tools used to model the different types of data collected, and to measure information imperfections as well as redundancy and complementarity will be described as follows:

1) Complementarity

It is the property of data sources (observer nodes) which provide information on different quantities. It comes from the fact that they generally do not give information on the same characteristics of the phenomenon observed. (Example the Hop Count and PDR). It is exploited by the data preprocessing method to have more complete global information and to remove ambiguity.

2) Ambiguity

It expresses the ability of relevant information or a parameter to lead to two interpretations. It can come from the

Contribution and Proposed Approach	Method used	Detection methods	Routing Protocol	Data Collector	Collected Data Type	Against Attacks
Routing anomaly detection in mobile ad hoc networks [13]	Markov chain, classifier construction and parameter tuning	ABIDS	DSR	Detection Agent	Change ratio of route entries and the number	active attacks: Routing Disruption
Towards Adaptive Intrusion Detection in MANETs [14]	Markov chain and parameter tuning	ABIDS	DSR	IDS Agent	New feature Link Change Rate (LCR)	Fake RREP packets Routing Disruption
A Intrusion Detection Scheme using SVMFN for MANETs [15]	Support Vector Machine and Fuzzy Integral	ABIDS	Routing	Several routing -related parameters	Local Data Collection Module (DCM)	Blackhole Attack
An Anti-Blackhole Mechanism (ABM) [16]	Predefined threshold value (Packet loss rates)	ABIDS	AODV protocol	IDS nodes	RREQs and RREPs messages	The selective Blackhole
Adaptive intrusion detection & prevention of DoS attacks in MANETs [17]	Statistical Process Control, Chi-square Test and Control Chart	ABIDS	AODV protocol	Head and Cluster Nodes (CH, CN)	Random Variables of Number of RREQs Received	Denial-of-Service (DoS)
An intrusion detection & adaptive response mechanism for MANETs[18]	Sliding Window Algorithm and Bernoulli Trial	both ABIDS and SBIDS	AODV protocol	Manager, Cluster, and Heads Nodes (MN, CH and CNs)	Network characteristic matrix (NCM) and Performance matrix (PM)	Blackhole, Grayhole, Sleep Deprivation and Rushing
Distributed and Cooperative Hierarchical IDS [19]	Data mining (CP-KNN) and DOD		AODV protocol	Attack Signature Database	Data Collection module (DCM)	Blackhole, Dropping Routing Traffic & Resource Consumption
An Intrusion Detection Tool AODVSTAT [20]	State Transition Analysis Technique (STAT)	SBIDS	AODV protocol	A node (i.e., an observer)	Traffic flows from its neighbors or collects UPDATE messages	Spoofing, Dropping packets and Resource epletion attack
Specification Synthesis for Monitoring and Analysis of MANET Protocols[21]	Inductive Logic Programming (ILP) method	SBIDS	AODV protocol	Form of a graph	Synthesized from the flow of the network traffic; Route request-reply flow	Attacks against routing protocols
Specification-based Intrusion Detection Model (SIDM) [22]	Previous Two Forwarders (PTF) method	SBIDS	AODV protocol	Node collects	HC, SN, RREQ identity, and IP address	Preventing a message field from being tampered
Detection of application-layer tunnels [23]	rules-based DGA and machine learning algorithm	both ABIDS and SBIDS	HTTP HTTPS DNS protocols	Virtual Private Server	Packet size (length) , arrival time and number (count)	Application -layer tunnels
Adaptive security-related data collection [24]	Data Description Language (SDDL)	—	VoLTE communication data	Data collector	Hash File -	Network attacks

Table 1: An overview of Data Collection Methods

following imperfections, for example from the imprecision of a measurement which does not make it possible to differentiate two situations, or from the incompleteness which induces possible confusion between results and situations which cannot be separated according to the characteristics highlighted by the source. One of our primary objectives is to remove the ambiguities of a source thanks to information provided by other nodes or by additional knowledge (calculates the PDR).

3) Incompleteness

Incompleteness characterizes the absence of information provided by a mobile node. The information provided by some node is generally partial; it provides only a vision of the phenomenon observed, by highlighting only certain characteristics.

4) Imprecision

Imprecision concerns the content of information on mobile nodes present from collected data. It concerns the lack of accuracy in quantity, in duration, the lack of definition of a proposal which is open to various interpretations or which has vague and ill-defined boundaries. This notion is often wrongly confused with that of uncertainty, because the two imprecision and uncertainty are often present simultaneously, and one can induce the other. Therefore, it is important to distinguish them because they are often antagonistic, even if these two terms can be included in a broader meaning of uncertainty.

5) Uncertainty

Uncertainty is relative to the truth of the metrics obtained from the data collected. It refers to the nature of the mobile node or of the fact concerned, to its quality of service, to its movement in the mobile network. The most common distinction in the literature is to divide uncertainties into two types: random uncertainty and epistemic uncertainty. The first being irreducible and due to the natural variability of random phenomena. The second is due to a lack of

knowledge, which can be reduced by making more efforts. However, there are other classifications of uncertainties because the random/epistemic classification is not rich enough for practical decision-making. The authors [25] define uncertainty in three dimensions. Blurred level, incomplete level and Random level. This has led to a distinction between these three levels of uncertainty. However, the behaviors collected from mobile nodes will be treated in such a way as to generate attack behavior, while respecting the conflicts of metrics obtained from the collected data.

6) Conflict:

Conflict characterizes two or more network parameters leading to contradictory and therefore incompatible interpretations. Information from collected data is more directly related to the observation conditions. Often, these types of information have distinct specification. Their resolutions can take different forms. They can be based on eliminating redundancies, taking into account additional information, etc.

7) Redundancy

Redundancy is the quality of sources (observer nodes or IDS nodes) which provide the same information several times (example of acknowledgment in the AODV). The redundancy between the source nodes is often observed, insofar as the sources give information on the same phenomenon. The elimination of redundancy is exploited to reduce the uncertainty and imprecision of collected data.

III. Intrusion Detection architecture for MANET

The purpose of undertaking this study is to improve the data collection mechanism of generating an efficacy labeled dataset with relevant data uncertainty. Moreover, we highlight the relevant features that distinguished the intruder and define the rules or patterns that identify attacks or classes of intruders in MANET. Accordingly, we introduce an optimization model for the IDS dedicated to MANET in an uncertain context (see Figure 2). In providing further clarification, we presented the approach from the related work that connected with our proposition, which is a recent paper [27], [28]. In [27], the authors present three algorithms for building an evaluation dataset for detecting. DoS attacks. In [28], the authors utilize a labeled dataset to increase the intrusion detection system performance and accuracy. The principal differences between this proposed approach and the previous work are that we focus on the data collection to improve the Labeled dataset, which is the most massive uncertainty. We aim, in this proposed approach, to determine data collection procedures that enhance the quality of the data collection and put in place data collection techniques that lead to the improvement of the Labeled datasets used in the security challenges in MANETs.

A. Data Collection

Data Collection shows the processed traffic collection and abstraction in dynamic and in an uncertain context. Due to the specificity of the mobile network, the mobile nodes communicate within wireless links.

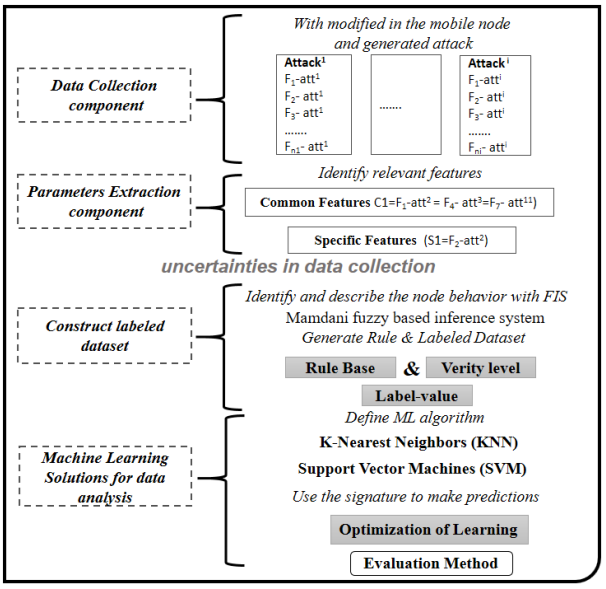

Figure. 2: Optimization Model IDS for MANET

Each mobile node can work as a sender, a receiver or a router. During the data collection process, the network cannot guarantee the same route to reach the selected destination route. Accordingly, we need some supplementary nodes. Two kinds of mobile nodes are considered. The first one's group include the mobiles nodes that will be utilized as a router to forward data packets. The second one's group encompass the mobiles nodes with special capacities that are utilized to collect data for the Intrusion Detection System. To trust the integrity of the collected data, these IDS nodes are supposed to be protected. These specifics nodes are both forms used as and the data collection node and the routing node. In the network monitoring process, IDS node monitors the mobile network and collects audit data specific for neighbors nodes in the network. The data are collected in the form of Node and Network Characteristic Values (NCF). A current dataset forms a dataset that contains all traffic that goes through different network interfaces. All these collected data are described in this NCF dataset. We processed the features of the data collection by the Data Preprocessing process [5]. We try to select useful features to define the malicious nodes in the next section.

B. Parameters Extraction component

When searching for the effectiveness of detecting variants of the same attack, this raw data does not give a multivariate signature for each attack. We consider this data will be presented in a vector of Features Attacks are defined as follows: FA (att_1) =< F1-att_1, F2-att_1 …Fn-att_1 >. With n belongs to N is the number of Features that define by the malicious node (example by the attack att1). We can distinguish two types of Features: The Basic Features can withstand several types of attacks but cannot differentiate and classify the type of malicious node. For example, the end-to-end delay: this is the time taken to transfer a packet between two nodes. In the case where the source sends its packets at maximum speed and the destination processes, each packet as soon as it arrives. In this stage, this metric cannot be taken into consideration as a relevant parameter to define and determine the type of malicious node. These features will be presented in a vector of the Basic Features

Attacks are defined as follows: BFA (att_1) =<C_1, C_2...C_j> with j belongs to N. While a Specific Features Attacks are defined as follows: SFA (att_1) =< S_1; S_2...S_k> can be differentiated and specify the nature of the attack. With k belongs N is incremental for each new functionality detected. Using the Hop Count metric example, this is the number of hops required to reach the destination. It favors paths with a small number of hops but it also tends to favor long distance links, which can offer low powers of the received signal and high packet loss rates. Based on this metric, we can detect most denial of service attacks. We will consider this metric as a relevant parameter. Therefore, for each attack we can identify two types of metrics, either Basic Features or Specific Features. Similarly, we can determine the Common Features of several attacks are defined as follows: C_j =<SFA (att_1) = SFA ($att_{(i\ \ 1)}$ = SFA (att_i) >follows Sk(att_1) =< Fn att_1 >. Otherwise, we can define: FAi =<C_1, C_2...C_j>U<S_1, S_2...S_k>. To and the Specific Features by particular attack are defined as identify and normalize the specific metrics for each attack, all the specific Features SFA have as relevant Features.

C. *Measurement Uncertainties*

We have touched on a few points dealing with the gaps in our dataset such as Uncertainties and inaccuracies are inherent, and have their origin at different levels: data observation phenomena, the mobile data acquisition system, the metrics disseminated by the protocol of routing to manage the problem of mobility, etc. All of these uncertainties can lead to high packet loss rates in the presence of mobility. Inaccuracies are then influenced in the construction of a reliable behavioral base and on which rely on the intrusion detection rate. Indeed, the fuzzy sets interpret the uncertainty in an approximate way. The theory of fuzzy sets allows an object to belong to several exclusive sets within the framework of reasoning. Each set has a degree of certainty that an object belongs to a fuzzy set. Fuzzy logic is based on the concept of fuzzy subsets, as opposed to binary logic. This makes it possible to take into account and manipulate data of an imprecise nature, classes with vague and possibly uncertain borders that can overlap, or even the notion of multi-membership of an element with several classes with a certain degree. In addition to all of these fundamental concepts, fuzzy reasoning reconciles, in a coherent way, symbolic or qualitative data with numerical data [26]. The interest of fuzzy sets for processing the relevant behaviors of a mobile node can be declined in particular according to the following three aspects. The capacity of the fuzzy sets to represent the information of a behavior of the mobile nodes as well as its imprecision, on various levels (normal behavior of the mobile nodes or well abnormal), and under various forms (numerical, qualitative, quantitative). The possibility of generalizing to fuzzy sets of operations manipulates the collected database knowing that the information is incomplete, vague, and imprecise. The possibility of representing very heterogeneous information, extracted which were by the relevant behaviors in order to identify the mobile nodes in MANET [28].

D. *Construct labeled dataset*

Our primary interest is to establish a data collection to generate a labeled dataset as a basis for identifying suitable IDS datasets, given specific evaluation scenarios for mobile networks. Given a labeled dataset in which each data is attached to the class normal or intruder, the number of detected malicious nodes or the number of false alarms may be utilized as evaluation criteria in intrusion detection. The dataset features Labeled are the most decisive features when searching for adequate network-based datasets. In this case, we aim to describe a labeled dataset, a thorough study of attacks and a selection of the several recent Denial of Service attacks against MANET. The research will be reduced to four types of DoS attacks; Blackhole, Grayhole, Wormhole, and Flooding attack. The SFA is needed to achieve the impact of the attack on routing behavior and network topology. We mainly evaluate the relevant features beginning from NCF dataset [28]. We consider Average in the RREQ packet of Sequence Number (*SN*), Hop Count (*HC*), Data Packet Dropped Rate (*DPDR*), and Packet Delivery Ratio (*PDR*). We describe the features using these performance metrics. We consider that the FIS will examine these measures. Let us take our NCF dataset where a scenario is classified based on their behavior. Based on Multi-Label Classification, each data collection scenario could appropriate in one of the behavior node categories. Therefore, each fuzzy input value of the crisp input can be assigned with one category. Therefore, the labeled dataset can be explained by each pattern of signatures in a unique value. The dataset should contain the label values of data points from each class labels. To train and evaluate malicious behavior, we require labeled-NCF dataset is required.

E. *Machine Learning for data analysis*

Machine learning (ML) is a method of data analysis that automates analytical model building. ML can be used for Anomaly Detection in Mobile Ad-Hoc Networks. In this paper, we adopted learning algorithm to predict the malicious nodes in Mobiles Networks. It aims to find a balance between the complexity of the model and its learning ability. The model presented by the supervised machine learning process can make predictions on new data values. We apply a Support Vector Machine and K Nearest Neighbor (KNN) for learning. The supervised algorithm is employed to determine the most optimal dataset; the NCF dataset compared with Labeled-NCF dataset (Fuzzy-KNN and Fuzzy-SVM). The good performance of the suggested model can be explained by the selection of an adequate classification supervised algorithm. In order to apply a learning algorithm, we split our dataset into two parts: a training and test dataset. The former is applied to make a model and train it. The latter is new data in which output values are withheld from the algorithm. We gather predictions from the trained model on the inputs from the test dataset and compare them to the withheld output values of the test dataset. Comparing the predictions and withholding outputs on the test dataset allows us to compute a performance measure for the model on the test dataset. We also made use of cross-validation is used to explain and analyze the performance of the security system proposed. In this situation, we split the dataset is split into ten datasets (k=10), of which ninety per cent for the training phase and ten per cent were employed in the testing phase. In the measurement through the performance for the IDS, we replicated this process for the calculation of the detection rate for normal and abnormal behavior.

IV. Experiments and results

The method to the Network-based in Mobile Ad-Hoc network with AODV protocol is applied. The experimental measurements of relevant performance metrics are used to mark the highlights of the mobile network with normal and abnormal behavior in MANET. In addition, different metrics were considered with the average values for various simulation times and different simulation scenarios. The simulation study is investigated using Opnet Modeler 14.5 simulator. (See Table 2) We assume that a MANET contains two or more mobile devices. Depending on the several types of Denial of Service attacks, we modified and implemented in Mac layer of the Mobile Ad-Hoc Network with AODV routing protocol. The normal profile is collected with the absence of any malicious node. However, the attack profile is created by simulating the malicious nodes. In this case, it is possible to identify the pattern of each attack. The NCF dataset contains a total of 1510 samples belonging to 5 different classes. For each one class; we collected the audit data specific for neighbors of mobile nodes. The sample distributions for different categories will be given to 302 samples for each class.

Parameters	**Definition / Value**
Version	Opnet Modeler 14.5
Number of Mobile Nodes	50 mobiles nodes
Transmission Range	250 m
Routing Protocol	AODV Protocol
Application Protocol	FTP and HTTP Protocols
Simulation Area Size /topology	1 Km x 1 Km
Simulation Duration	60 minutes
Node Placement (Mobility)	Random Waypoint
Mobility Malicious Nodes	2 to 6 mobiles nodes
Channel type	Wireless channel
Mac Layer	Wireless LAN Mac
Traffic Sources (Type)	CBR (UDP)
Size of Data Packet	512 bytes

Table 2: Opnet configuration parameters

In this section, we will illustrate some experimental results. Refereeing back to the recent papers by MEDDEB et al [5], [27], and [28], we presented the approach from related work, which goes hand in hand with our study. In fact, it is worthy to mention in [27] that the authors perform three algorithms in order to build up a dataset for IDS through Fuzzy Inference System use. Hence, they do carry on within the process to generate an intrusion detection datasets for detecting malicious nodes. Besides, explaining the malicious activity seems to be inter-linked with the application as well as the identification of the FIS via the security of the mobile node behavior. Furthermore, in [5] the authors refer back to the use of preprocessing data to reach a particular improvement regarding the precision as well as the classification. Added to that, we resorted to a Machine Learning algorithm, which can be applicable and doable in malicious nodes detection [28]. The goal behind our study is slightly non-similar to the prior highlighted approaches in one pertinent focus, which turns around the use Mamdani type for the FIS. The verity level checks the behavior of a node whether to be normal or malicious on the bases of uncertainty relevant features. The main difference between this approach and the previous work to improve the data collection mechanism of generating an efficacy labeled dataset with data uncertainty relevant. In order to determinate, the most optimal Labeled dataset we need to apply the Supervised Machine Learning algorithm and to put under scope the NCF dataset (KNN) compared with Labeled-NCF dataset (Fuzzy-KNN) and Labeled-NCF dataset (Fuzzy-SVM). Hence, our evaluation labeled dataset is split into training and testing data with a 90-10 split. The training data consists of 90% of total instances, as for testing data, it contains 10% of the total instances. However, performance measures for intrusion detection can be checked in summary of prediction. As for the Table 3, it represents comparison with previous accomplish work. We can deduct that the indicators, which had been relied on, are performance metrics; i.e. Sensitivity (Se), Specificity (Sp), Positive Predictive Value (PPV), Negative Predictive Value (NPV), Accuracy and the Balanced Accuracy. For the sake of understanding via the bias of the proposed detector towards a well-picked class of malicious nodes (Blackhole, Grayhole, Wormhole and Flooding Attacks) and the normal behavior. The forecast results vary in different classes.

Predicted/Actual	Se	Sp	PPV	NPV	Accuracy
Normal	1.000	1.000	1.000	1.000	1.000
Blackhole	1.000	**0.900**	**0.714**	1.000	**0.950**
Grayhole	**0.900**	1.000	1.000	**0.975**	**0.950**
Wormhole	0.700	1.000	1.000	**0.930**	**0.850**
Flooding	1.000	1.000	1.000	1.000	1.000
Balanced Accuracy Fuzzy					**0.92**
Normal	1.000	1.000	1.000	1.000	1.000
Blackhole	1.000	**0.912**	**0.734**	1.000	**0.950**
Grayhole	**0.860**	1.000	1.000	**0.952**	**0.920**
Wormhole	0.700	1.000	1.000	1.000	**0.860**
Flooding	1.000	1.000	1.000	1.000	1.000
Balanced Accuracy KNN					**0.92**
Normal	1.000	1.000	1.000	1.000	1.000
Blackhole	1.000	**0.925**	**0.769**	1.000	**0.962**
Grayhole	**1.000**	1.000	1.000	**1.000**	**1.000**
Wormhole	**0.715**	1.000	1.000	1.000	**0.870**
Flooding	1.000	1.000	1.000	1.000	1.000
Balanced Accuracy Fuzzy-KNN					**0.94**
Normal	1.000	1.000	1.000	1.000	1.000
Blackhole	1.000	0.977	0.909	1.000	0.988
Grayhole	**1.000**	0.977	0.909	**1.000**	**0.988**
Wormhole	**0.850**	0.857	1.000	1.000	**0.928**
Flooding	1.000	1.000	1.000	1.000	1.000
Balanced Accuracy Fuzzy-SVM					**0.96**

Table 3: The results of the performance measures

As an interpretation, we can deduce that the detection of normal behavior represents no trouble to us as it is frequently ranked under 100%. However, there is a specific variation for the Denial of Service attacks according to the attack types as well as the data analysis method. We can conclude that the detection of Flooding attack allowed a high detection rate, which is frequently ranked under 100%. Concerning the Blackhole attack, Accuracy faces no change between the Fuzzy Inference or KNN algorithm. Its Balance Accuracy only reached 92%. Thus, when we joined both methods, i.e. Fuzzy Inference and KNN, the accuracy value reaches 96.2%. This is due to the enhancement that took place with regard to the Specificity of 92.5% and Positive Predictive Value of 76.9%. The Accuracy of this attack performed well in SVM classifier with 98.8% due to the higher value of the Specificity 97.7% and the Positive Predictive Value of 90.9%. As for the Detection rate for Grayhole attack with Fuzzy Inference System, it is archived only at 95%, due to reaching 90% of Specificity value and 97.5% of Negative Predictive

Value. However, in KNN classifier the detection rate is only 92% and the Negative Predictive Value is 95.2%. Moreover, there is an improvement in the detection rate for this malicious node is reaching 100% of Accuracy with Fuzzy-KNN whereas in Fuzzy-SVM it achieved only 98.8%. Wormhole attack represents one form of Dos attack, which is the most delicate and hard to detect. The detection rate obtained by Fuzzy-SVM classifier shows better results than Fuzzy-KNN, KNN, and Fuzzy Inference System i.e., the Balance Accuracy is 85%, 86%, 87%, and 92.8%, respectively. However, the accuracy of Wormhole with the Fuzzy-SVM needs further study. Besides, the predicted value of this malicious node is highly noticed. We define these as follows two malicious nodes construct a link. If this tunneling is accomplished without any malicious intention, the attacker actually guarantees connections that are more efficient in the mobile network. Nevertheless, the powerful position of a malicious node can be applied in a kind of ways, such as packet dropping or data modification. This malicious node selects the route, which contains an attack. Since it has a much higher probability of packet dropping, we can come to an end, which is that the Fuzzy Inference System followed by the data analysis using the machine learning gives us a higher rate Accuracy detection compared with the FIS only. One the Balanced Accuracy equal to 92% we directly apply the Fuzzy Inference System or only KNN algorithm. Hence, the Fuzzy-KNN classifier, which was trained and tested, reached a Balanced Accuracy of a higher rate, i.e. 94%. It is interesting to the highlight an important point, which is that the Fuzzy-SVM classifier was trained and tested to reach a Balanced Accuracy of 96%. Our simulation result prove that the proposed Fuzzy-SVM is more capable of detecting specific malicious nodes (DoS attacks) with a lower false positive rate and a higher true positive rate. This result proves the fact that an IDS trains a sequence of models. The Fuzzy-SVM classifier shows better performance in some malicious nodes and the accuracy varies between 92% and 100%.

V. Conclusion

Mobile Ad-Hoc Networks are used in many fields and require providing effective advanced security. Therefore, a defensive mechanism against attacks should be designed. Our approach implements a data collection and data analysis method with uncertainty parameters (data collected) for reliable analysis of the dataset labeled in MANETs. Based on our results, we identify some issues that remain open for the purpose of future research in the area of intrusion detection in Mobile Ad-Hoc Networks. In some MANET deployments, the network tries to extend the notions of mobility to all components of the environment. The latter can consist of hundreds or thousands of mobile nodes. Under these conditions, no limitation or assumption is made on the extensible structure of the network and the huge size of collected data. In the greatest majority of existing mechanisms, collectors nodes collect all the network data flow. However, not all of these nodes are needed for the corresponding data collected or analysis process. Indeed, the IDS node is too heavy and do not collect or manage useless data due to the limited memory and resource consumption at collectors mobile nodes. Nevertheless, the literature still lacks an intrusion detection dataset with high effectiveness and accuracy, as well as adaptability form a large number of dynamic and autonomous nodes. Therefore, the issues of collected data amount are still open for future researchers.

Acknowledgments

This work has been done as part of the Tunisian National Research Project PACTE-Profiler.

References

[1] Rath, M. Big data and iot-allied challenges associated with healthcare applications in smart and automated systems. *International Journal of Strategic Information Technology and Applications*, 9(2), pp. 18-34, 2018.

[2] Meddeb, R., Triki, B., Jemili, F., Korbaa, O. A survey of attacks in mobile ad hoc networks. In *ICEMIS2017, Monastir, Tunisia (2017)*, pp. 1-6, 2017.

[3] Mekale, S.S., Saini, P.K., Batra, S. A Study on MANET Attacks, Security Concerns. *Journal of the Gujarat Research Society*, 21(16), pp. 2189-2194, 2019.

[4] Laqtib, S., El Yassini, K., Hasnaoui, M.L. A technical review and comparative analysis of machine learning techniques for intrusion detection systems in manet. *International Journal of Electrical and Computer Engineering*, 10(3), pp. 2701-2709, 2020.

[5] Meddeb, R., Jemili, F., Triki, B., Korbaa, O. Anomaly-based behavioral detection in mobile ad-hoc networks. *Procedia Computer Science*, 159(1), pp. 77-86, 2019.

[6] Kumar, S., Dutta, K. Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges. *Security and Communication Networks*, 9(14), pp. 2484-2556, 2016.

[7] Lin, H., Yan, Z., Chen, Y., Zhang, L. A survey on network security-related data collection technologies, *IEEE Access*, 6(1), pp. 18345-18365, 2018.

[8] Yan Z. Network Data Collection, Fusion, Mining and Analytics for Cyber Security, in *Machine Learning for Cyber Security* , Chen X., Huang X., Zhang J. (eds.), Machine Learning for Cyber Security, Springer, 2019.

[9] Zhou, D., Yan, Z., Fu, Y., Yao, Z. A survey on network data collection. *Journal of Network and Computer Applications*, 116(1), pp. 9–23, 2018.

[10] Hussain, M.S., Khan, K.U.R. A survey of ids techniques in manets using machine learning. in *the Third International Conference on Computational Intelligence and Informatics*, Raju K., Govardhan A., Rani B., Sridevi R., Murty M. (eds.) Advances in Intelligent Systems and Computing,, Springer, Singapore, 1090, pp. 743-751, 2020.

[11] Liu, G., Yan, Z., Pedrycz, W. Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. *Journal of Network and Computer Applications*, 105(1), pp. 105-122, 2018.

[12] Magan-Carrion, R., Urda, D., Daz-Cano, I., Dorronsoro, B. Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches. *Applied Sciences*, 10(5), pp. 1775-1796, 2020.

[13] Sun, B., Wu, K., Pooch, U.W. Routing anomaly detection in mobile ad hoc networks. In *12th*

International Conference on Computer Communications and Networks, pp. 25-31, 2003.
[14] Sun, B., Wu, K., Pooch, U.W. Towards adaptive intrusion detection in mobile ad hoc networks. In *IEEE Global Telecommunications Conference, 2004. GLOBECOM04*, pp.3551-3555, 2004.
[15] Li, H., Gu, D. A novel intrusion detection scheme using support vector machine fuzzy network for mobile ad hoc networks. In *2009 Second Pacific-Asia Conference on Web Mining and Web-based Application, IEEE*, pp. 47-50, 2009.
[16] Su, M.Y. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, 34(1), pp. 107-117, 2011.
[17] Nadeem, A., Howarth, M. Adaptive intrusion detection & prevention of denial of service attacks in manets. In *Proceedings of the 2009 international conference on wireless communications and mobile computing: Connecting the world wirelessly, ACM*, pp. 926-930, 2009.
[18] Nadeem, A., Howarth, M.P. An intrusion detection & adaptive response mechanism for manets. In *Ad Hoc Networks*, 13 pp. 368-380, 2014.
[19] Abdel-Fattah, F., Dahalin, Z.M., Jusoh, S. Distributed and cooperative hierarchical intrusion detection on manets. In *International Journal of Computer Applications*, 12(5), pp. 32-40, 2010.
[20] Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E.M., Kemmerer, R.A. An intrusion detection tool for aodv-based ad hoc wireless networks. In *20th Annual computer security applications conference, IEEE*, pp. 16-27, 2004.
[21] Stakhanova, N., Basu, S., Zhang, W., Wang, X., Wong, J. Specification synthesis for monitoring and analysis of manet protocols. In *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW07), IEEE*, pp. 183-187, 2007.
[22] Lin, H.C., Sun, M.K., Huang, H.W., Tseng, C.Y.H., Lin, H.T. In *A specification based intrusion detection model for wireless ad hoc networks. 2012 Third International Conference on Innovations in Bio-Inspired Computing and Applications, IEEE*, pp. 252-257, 2012.
[23] Lin, H., Liu, G., Yan, Z. Detection of application-layer tunnels with rules and machine learning. in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Wang G., Feng J., Bhuiyan M., Lu R. (eds.), SpaCCS, LNCS 11611, pp. 441-455, 2019.
[24] Lin, H., Yan, Z., Fu, Y. Adaptive security-related data collection with context awareness, *Journal of Network and Computer Applications*, 126 (1), pp. 88-103, 2019.
[25] Blockley, D. Analysing uncertainties: Towards comparing bayesian and interval probabilities. *Mechanical Systems and Signal Processing*, 37 (1), pp. 30-42, 2013.
[26] Ishibuchi, H., Yamamoto, T., Nakashima, T. An approach to fuzzy default reasoning for function approximation. *Soft Computing*, 10(9), pp. 850-864, 2006.
[27] Meddeb, R., Triki, B., Jemili, F., Korbaa, O. An effective ids against routing attacks on mobile ad-hoc networks, in *New Trends in Intelligent Software Methodologies, Tools and Techniques - Proceedings of the 17th International Conference SoMeT 18*, H. Fujita and E. Herrera-Viedma (eds.), 297., IOS Press, pp. 201-214, 2018.
[28] Meddeb, R., Triki, B., Jemili, F., Korbaa, O. Dataset for intrusion detection in mobile ad-hoc networks. In*19th International Conference on Intelligent Systems Design and Applications, ISDA 2019*, pp. 10-20, 2019.

Author Biographies

Rahma MEDDEB received the Engineering Diploma in Computer Science and Telecommunications form Higher Institute of Computer Science and Telecom of Hammam Sousse (ISITCom-University of Sousse) in 2011. Currently, she is a PhD Student in Computer Science in the same Faculty. She is a member of MARS Research Laboratory (ISITCom-University of Sousse), since 2015. Her research interests include the treatment of digital investigation of security incidents, intrusion detection systems, security and privacy issues and Artificial Intelligence and Data Analysis.

Dr. Bayrem TRIKI received the Ph.D. in Telecommunications from the Engineering School of Communications (Sup'Com), University of Carthage (Tunisia) in 2013. He is currently an Assistant Professor in Institute of Computer Sciences and Communication Techniques (ISITCom) at the University of Sousse. Dr Triki conducting research activities in of digital investigation of security incidents, intrusion detection systems, Internet of Things security and privacy issues, Cloud computing and network attacks.

Dr. Farah JEMILI holds a MSc in computer engineering (2002) and PhD with honor in computer sciences (2010). She is currently Assistant Professor at Higher Institute of Computer Science and Telecom of Hammam Sousse (ISITCom-University of Sousse) and Senior Researcher at MARS Laboratory (ISITCom University of Sousse). She has extensive experience as a researcher in Artificial Intelligence, Big Data Analysis and Distributed Systems with special focus on Intrusion Detection Systems. She has many publications and served as reviewer for many international conferences and journals.

Pr. Ouajdi KORBAA obtained in 1995 the Engineering Diploma from the Ecole Centrale de Lille (France), and in the same year, the Master degree in Production Engineering and Computer Sciences from the University of Lille I. He is Ph.D. in Production Management, Automatic Control and Computer Sciences of the University of Sciences and Technologies of Lille (France) since 1998. He also obtained, from the same university, the Habilitation to Supervise Researches degree in Computer Sciences in 2003. He is full Professor in the University of Sousse. He published around 140 research papers on scheduling, performance evaluation, discrete optimization, design, and monitoring.