
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issue 1, pp. 137–145, DOI 10.12694:/scpe.v21i1.1642

A HYBRID INTRUSION DETECTION SYSTEM FOR MOBILE ADHOC NETWORKS USING FBID PROTOCOL

D. RAJALAKSHMI *AND K. MEENA †

Abstract. A Security in a mobile ad hoc networks is more vulnerable and susceptible to the environment, because in this network no centralized environment for monitoring individual nodes activity during communication. The intruders are hacked the networks either locally and globally. Now a day's mobile ad hoc network is an emerging area of research due to its unique characteristics. It's more vulnerable to detect malicious activities, and error prone in nature due to their dynamic topology configuration. Based on their difficulties of intrusion detection system, in this paper proposed a novel approach for mobile ad hoc network is Fuzzy Based Intrusion Detection (FBID) protocol, to identify, analyze and detect a malicious node in different circumstances. This protocol it improves the efficiency of the system and does not degrade the system performance in real time. This FBID system is more efficient and the performance is compared with AODV, Fuzzy Cognitive Mapping with the following performance metrics: Throughput, Packet Delivery Ratio, Packets Dropped, Routing overhead, Propagation delay and shortest path for delivering packets from one node to another node. The System is robust. It produces the crisp output to the benefit of end users. It provides an integrated solution capable of detecting the majority of security attacks occurring in MANETs.

Key words: Security, Intrusion detection, AODV, MANET, Fuzzy, Cognitive Map

AMS subject classifications. 68M15

1. Introduction.

A Mobile adhoc network is a complex wireless network, it consist of collection of mobile nodes, which forms a spontaneous network without the physical infrastructure, it allows individual, group of members and organizational members work together and communicate without the stable infrastructure [1]. Limitation of mobile adhoc networks are bandwidth and energy consumption.

A mobile adhoc network is shown in cf. Fig.1.1. It's an infrastructure less network because the mobile nodes in the network dynamically change the paths with other nodes and transmit the data packets provisionally. In a MANET, nodes within the region or specified boundary means, it communicates with other nodes directly, otherwise it needs to rely on some other nodes to relay the messages from source to destination. The major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. There are confidentiality, availability, non-repudiation, authentication and integrity. The security attacks in MANET can be roughly classified in two types: 1) Active Attacks and 2) Passive Attacks.

Hosts may misbehave or try to compromise security at all layers of the protocol stack. In Transport layer to provide secure end-to-end communication [2]. For that need to know keys to be used for secure communication, then it anonymity the communication. In Network layer, the misbehaving hosts may create the hazards; in terms of it disrupt the route discovery and maintenance. Due to that hazard, Delay, drop, corrupt and misroute the packets. It degrades the networking performance. In MAC layer, the misbehaving nodes may not cooperate to each other. Because disobey the protocol specifications for selfish gains.

Mobile Ad hoc networks are collections of mobile nodes that may enter and leave the network dynamically. No centralized controller and infrastructure. A major issue in Mobile ad-hoc network is security. This also aims of the work in MANET. To detection of malicious nodes forms a very essential one of the part an approach to security [3]. The main objective of this work is to detect the intrusions through Fuzzy logic that prevents the network from denying the active session or extract the confidential information that is being shared. The

*Research Scholar, Vel Tech Rangarajan Dr. Sagunthala R and D Institute of Science and Technology, Chennai. Assistant Professor, Sri Sairam Institute of Technology, Chennai, India (rajisacet@gmail.com).

†Professor, Vel Tech Rangarajan Dr. Sagunthala R and D Institute of Science and Technology, Chennai, India.

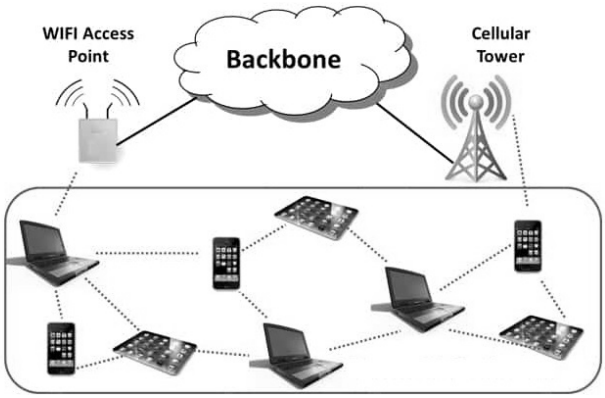

FIG. 1.1. *Mobile Ad hoc Network*

proposed work uses FBID to identify the malicious nodes of capture the intrusion over MANET that networks as well as provide the best solution to reduce the execution time over the network[4].

2. Related Work. Security is an essential requirement of mobile adhoc networks. These networks are more vulnerable and threats are increased due to lack of security and very hard to implement the centralized security control for authentication purpose [5]. The main attributes of security requirement of mobile adhoc networks are [6]:

Confidentiality: It has a set of rules; it limits the unauthorized users accessing the network.

Data Integrity: It gives the information as trustworthy and accurate data.

Availability: It's reliable access to the authorized users.

Denial of Service: It is attacked by malicious nodes or selfish nodes.

The characteristics of Mobile Adhoc Networks are:

Dynamic Topologies: Randomly the network topology has changed, and inside the node also moving freely with different speed at changeable times.

Energy - Constrained Operation: In wireless networks the individual node rely on batteries, entire energy is drained due to continuous monitoring or active in all times till the energy has exhausted.

Limited Bandwidth: In wireless communication the signals or data's are dropped due to noise, interference, fading, multiple accessing technique and weather conditions. If the data's are dropped then automatically the throughput has reduced and it leads to the less bandwidth consumption.

Security Threats: Security is lacking in wireless networks. Due to their infrastructure less network any one can hack the system in the form of passive attacks and active attacks.

The challenges of Mobile Adhoc Networks are [7]:

Scalability: To measure the performance of network, the scalability is the main issue. How many packets or data to be delivered to the particular destination without data loss, it can be measured by scalability. Now a day the overall performance of the network is based on throughput, it is low in wireless environment. For this improvement, crucial research work is progress on.

Quality of Service: Need to improve the quality of service robustness, algorithms, protocols and policies to be addressed in a very effective manner in wireless region. Quality of service can be measured by the following factors: Delay, Jitter, Bandwidth and Throughput [8].

Client–Server Model Shift: In wireless domain, Client - Server concept is not applicable in real time, because there is no stable state for server, connections, IP addresses and authorization mechanisms. Here the individual node may act as a client or server, that is, peer-to-peer communication. For this purpose the traditional client-server model to be implemented in a better way for wireless communication.

Security: In Mobile adhoc networks the suspicious or malicious node they can enter the network, and compromise the network. The individual nodes are dynamically moving at irregular time intervals; in that case the malicious nodes are attacking the network and observing the nature of data [9].

Interoperation with the Internet: Now a day without internet we cannot do anything. In mobile adhoc networks the configuration and set up is differ from one network to another. The interface is main issue of connecting the different type of networks. It can be avoided by assigning foreign agent to the mobile IP.

Energy Conservation: Energy conservative networks are popular in adhoc networks. For better performance the entire battery is fully utilized for the active networks. Still the energy is constrained in wireless environment. It will be improved to implement a better routing algorithm for transmission and reception.

Node Cooperation: In wireless environment, the node cooperation is more important, because the individual nodes are independent; the malicious nodes are acting as a dependent node to all other nodes. These malicious nodes are charged in a very high manner and it consumes the entire battery power.

3. Problem Definition. In this paper, our objective is to solve the weakness of watchdog methods; Ambiguous collisions, Receiver Collisions, Limited Transmission Power, Partial Dropping, False Misbehavior Report and Collusion [10-11]. The Proposed work will be anomaly based intrusion detection system that is lack of monitoring capability and entering the malicious nodes inside the network. These issues are solved by fuzzy based intrusion detection protocol. The ultimate goal of the paper is finding the malicious node in effective way when compared to all other existing methods, measured by the following scenarios:

1. *Ambiguous Collisions:* In two nodes are communicated Node 1 and Node 2, it transmits a packet from node 1 to node 2 and vice versa, collision occurs in node 1 and node 2 it forward the packet. Node 1's collided by Node 2 transmissions, so neighbourhood nodes are not able to do the communication. Node 1 continuously monitors the same node, in this case malicious node accessed or hacking the network throughput.
2. *Receiver Collisions:* Two nodes are communicated say Node 1 and Node 2. The senders send a packet to Node 1 and monitor the action of node 1 and send the packet to node 2. Sender does not give any assurance to deliver the packet successfully at node 2. In this case collision occurs in node 2 means, again node 1 it resends the packet to node 2, due to number of times sending a same frame leads the malicious nodes it access the packet.
3. *Limited Transmission Power:* A misbehaving node consumes the transmission power, such that the signal is high in previous node or sender and too weak in the destination node. It leads to malicious node will enter and hack the network bandwidth.
4. *Partial Dropping:* In Watchdog mechanism, the packets are transmitted from one hop to another to reach the destination, but watchdog doesn't aware about where the packet reside in it and which hop to transfer the packet to the desired destination in the network. This lack of information leads to misbehaviour nodes are entered in the network; this also cannot be detected by watchdog. If it suspects the node become misbehavior, it forced to forward the packets to threshold bandwidth, and drops the packet.
5. *False Misbehavior Report:* The malicious nodes divert or falsely define the trusted node becomes misbehavior node. It diverts the monitoring controls to the trusted node. In that duration the malicious node access the network and grasp the information and leave the network.
6. *Collusion:* Multiple node collusion is well planned activity. For example two nodes are communicated say 1 and 2. It collides as due to malicious node. Here node 1 forwards the packet to node 2, but it not responds to the initiator, so node 2 it discards the packet. The consecutive untrusted nodes communicated in a single routing path. The Malicious node limits or spoils the communication.

4. Methodology. Due to the revolution of science and technology, it's more difficult to take decision and its leads to the issue of unclear or not expected results are generated, and it is very hard to analysed [12]. Fuzzy concept has the capability to take decisions in a correct manner through a formal mathematics and logic; it generates the qualitative data or predicted data. The fuzzy concepts are capable of handling humanistic type of problems.

The word fuzzy refers two things: true or false [13]. Any action or event, the current state is changed suddenly or continuously, it cannot be represented as either true or false. For this purpose, the fuzzy concept plays a vital role in emerging applications. In Boolean concepts the output is represented by 0 or 1[14 -15]. Fuzzy system values are defined in the range from 0 to 1 or yes/ no. But in fuzzy 1.0 represents "Absolute or

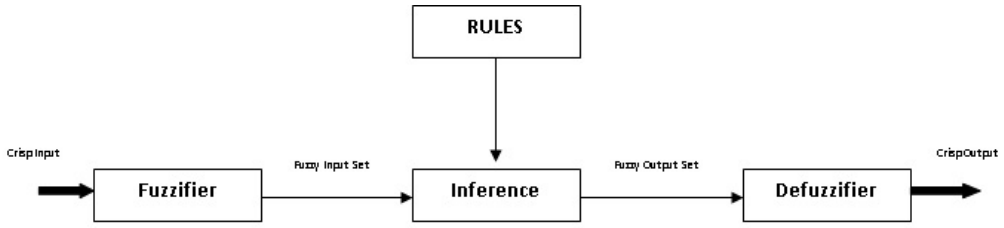

FIG. 4.1. *Fuzzy Logic Architecture*

extreme truth", 0.85 represents very truth, 0.35 represents sometimes truth, 0.0 represents absolute false. The range of fuzzy system is represented by the truth value. Fuzzy logic handles the reasoning capability with the fuzzy concepts. Fuzzy logic is a not a logic, it's a fuzzy, logic used to describe the fuzziness [16 -18].

The fuzzy set represents the one form of uncertainty. Suppose in regular activity of network, who are uncertain about the non malicious or innocence of the trusted node. The uncertainty in this situation it's very hard to find the malicious nodes and innocent nodes. In order to represent this type of uncertainty, assign a value to each possible crisp set [19]. This value defines the amount of confirmation or certainty of the nodes in that network. The uncertainty is also called as a fuzzy measure. Fuzzy measures solve the problem after considering all available data's, and then it takes the better relevant decision for the given input. It's shown in cf. Fig. 4.1.

There are four components of fuzzy logic architecture:

1. *Rules:* It contains set of rules and regulations that govern to take the better relevant decision making system. Due to the better relevant decision making system, it reduce the fuzzy rule.
2. *Inference:* It match the rules according the fuzzy input set, if it not matched with the existing rule, then the new rule will be implemented based on the fuzzy input. Afterwards the new rules are combined to take the better relevant decision.
3. *Fuzzifier:* Before entering to the inference process, we need the convert the crisp input in to fuzzy input set values. This conversion process is performed in fuzzifier.
4. *Defuzzifier:* It is used to convert the output of inference process, that is fuzzy output set into crisp output to the benefit of end users.

The benefits of Fuzzy logic systems are:

- Implementation of fuzzy logic system is easy and understandable.
- It provides a very efficient solution to the complex problems in the emerging trends.
- It deals with uncertainty in engineering.
- The system is robust.
- Easily modified to improve or enhance the system performance.

The limitations of Fuzzy logic systems are:

- Ambiguity: There is no systematic methods to solve the problems in real time issue.
- Lack of mathematical description: Proof of techniques is more complex and difficult to obtain for all possible scenarios.
- Verification and Validation is more complex.
- Don't have the capability of machine learning.

5. Performance Evaluation. Fuzzy Based Intrusion Detection System can be formed using two disjoint classes of fuzzy cognitive mapping. It has lot of advantages, cost-effective, perceptive and time consumption is very less. Fuzzy Based Intrusion Detection System is better than the normal fuzzy cognitive mapping, because here two disjoint zones are used to produce the better result in real time scenarios.

1. Region Zone
2. Field Zone

There are no intermediate relations are exist between Region and field zones. The numbers of elements are not mandatorily equal between these region and field zones. Region zone values are taken from the real vector

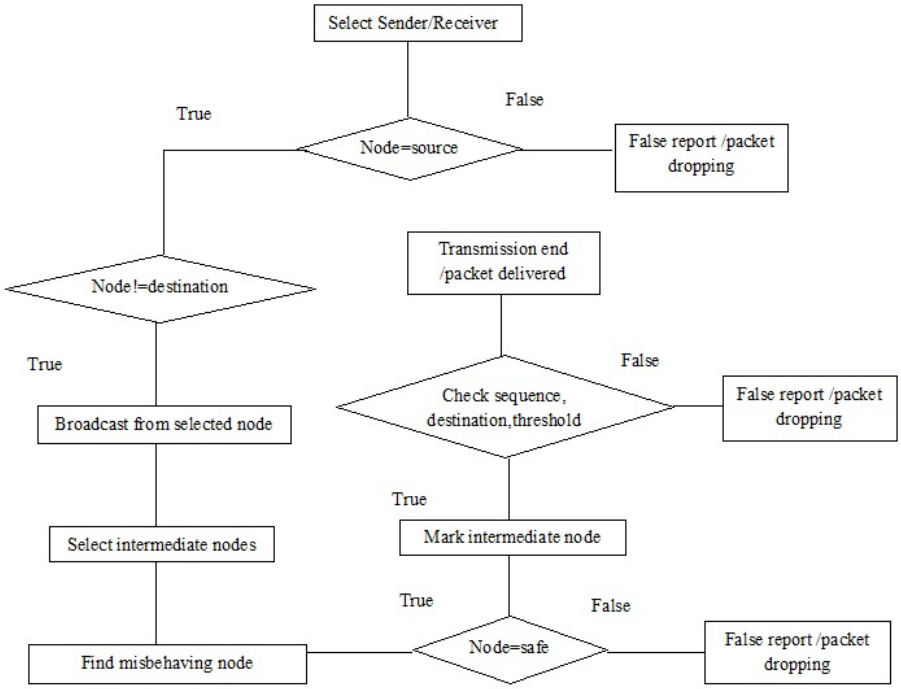

FIG. 5.1. *Intrusion Detection System*

zone of range represented by p and Field zone values are taken from the real vector zone of range represented by q. Set of zones are represented F, it has the dimension from $F_1, \ldots, F_m$ of the field zone, where F, range lies from a_1 to a_m, where $a_x = 1$ or 0 for $y = 1, 2, \ldots, s$. If $a_x = 1$ it means the zone F_i is in ON State and if $a_x = 0$ means OFF state. R denotes the zone $R_1, R_2, \ldots, R_n$ of the range zone, where R range lies from a_1 to a_n, where $a_x = 1$ or 0 for $x = 1, 2, \ldots, n$. If $a_x = 1$ it means the zone R_i is in ON State and $a_x = 0$ means OFF State.

Fuzzy Based Intrusion Detection System is a fixed graph; it represents the value of Region to Field zone with rule, conditions and policies, as zones and causalities as edges. It denotes the fundamental association between Zone R and F. When zones of the fuzzy based intrusion detection system are fuzzy sets it is also called as fuzzy zones. The weights zero, plus or minus one are called as simple fuzzy based intrusion detection system. The system architecture for intrusion detection is shown in Fig.5.1.

Let $R_1, R_2, \ldots, R_n$ be the zones of the region zone R of an FBID and $F_1, F_2, \ldots, F_m$ be the zones of the Field zone F of an FBID. Let matrix Z be defined as $Z = (z_{xy})$ where z_{xy} is the weight of the fixed edge $R_x F_y$, Z is called as the cognitive relational matrix of FBID.

Consider the relationship between the research work and scholar. Suppose the Region zone as perception is based on the research work say $R_1, R_2, \ldots, R_5$ and the field zone define the perception is based on the Scholar say $F_1, F_2, \ldots, F_5$. Let define the zones $R_1, R_2, \ldots, R_5$ and $F_1, F_2 \ldots F_5$ as follows. For Region Zone,
R_1: Research Work is Good.
R_2: Research Work is Poor.
R_3: Research Work is Average.
R_4: Research Work is Different Variety.
R_5: Research Work is not useful.
For Field Zone,
F_1: Good Scholar
F_2: Bad Scholar
F_3: Average Scholar

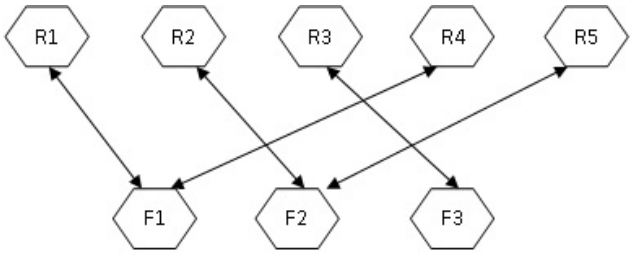

FIG. 5.2. *Cognitive relational fixed graph*

The cognitive relational fixed graph of the research work - scholar model is plotted in Fig 5.2.

The cognitive relational matrix Z derived from the above graph is:

$$Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{5.1}$$

If $C = (1, 0, 0, 0, 0)$ is passed on in the cognitive relational matrix Z, the instantaneous vector, $CZ = (1, 0, 0)$ implies that the scholar is a good scholar $CZ = D, DZ^{\mathrm{T}} = (1, 0, 0, 1, 0)$ implies that the research work is good and he/she did a research work is different variety. $DZ^{\mathrm{T}} = C_1, C_1Z = (2, 0, 0)$ after threshold, $C_1Z = (1, 0, 0)$ implies that the scholar is good, so on.

The Fuzzy cognitive relational membership is: If $C = (1, 0, 0, 0, 0)$ is passed on in the cognitive relational matrix Z, the instantaneous vector, $CZ = (1, 0, 0)$ implies that the scholar is a good scholar. $CZ = D, DZ^{\mathrm{T}} = (1, 0, 0, 1, 0)$ implies that the research work is good and he /she did a research work is different variety. $DZ^{\mathrm{T}} = C_1, C_1Z = (2, 0, 0)$ after threshold, $C_1Z = (1, 0, 0)$ implies that the scholar is good, so on.

The Fuzzy cognitive relational membership is:

$$\mu_x(R_i) = \begin{cases} 1 & \text{if Row sum of maximum value} \\ 0 & \text{if Row sum of minimum value} \\ \dfrac{R_i - \text{Row sum of minimum value}}{\text{Row sum of maximum value} - \text{Row sum of minimum value}} & \text{if Row sum of minimum value is less than or equal to } R_i \text{ and less than or equal to Row sum of maximum value} \end{cases}$$

$$\mu(x) = \begin{cases} \dfrac{(x-p)}{(q-p)} & \text{if } p \le x \le q \\ \dfrac{(r-x)}{(r-q)} & \text{if } q \le x \le r \end{cases} \tag{5.2}$$

μ is a fuzzy subgroup of CZ. Then $\mu(x^{-1}) = \mu(x)$ and $\mu(x) \le \mu(e)$ for all $x \in CZ$, where e is the identity element of CG.

$$\mu(x) = (\mu((x^{-1})^{-1}) \ge \mu(x^{-1}) \ge \mu(x))$$

Hence for $x \in CZ$,

$$\mu(e) = \mu(xx^{-1}) \ge \min(\mu(x), \mu(x^{-1})) = \mu(x)$$

TABLE 5.1
Analysis of AODV, FCM and FBID Protocol

Performance Metrics	AODV	FCM	FBID
Throughput	Moderate 60 to 75%	High 70 to 80%	Very High 80 to 90%
Packet Delivery Ratio	Moderate	High	Very High
Packets Dropped	Low	Low	Very Low
Routing Overhead	Less at moderate congestion	Low at reasonable congestion	Very low at less congestion
Propagation delay	Less at moderate congestion	Low at moderate congestion	Very low at less congestion
Shortest Path	Moderate	High	Very High

$$\mu(y) = \text{Max } [\text{Min } \mu_p k_1(\text{input}(i)), (\mu_p k_2(\text{input}(j))]$$

$$Z(x,y) = \begin{cases} \mu p(x) & \text{if } \mu q(y) = 1, \\ \mu q(y) & \text{if } \mu p(x) = 1, \\ 0 & \text{if } \mu p(x) < 1, \mu q(y) < 1 \end{cases} \tag{5.3}$$

$$Z(x,y) = \begin{cases} 1 & \text{if } \mu p(x) \leq \mu q(y) \\ \mu q(y) & \text{if } \mu p(x) > \mu q(y) \end{cases} \tag{5.4}$$

To maintain the consistensy using fuzzy logics, the probability is 1.

Degree of truth (T) + level of indeterminacy (I) + Degree of false (F) = 1

Incomplete information on a variable the proposition is:

Degree of truth (T) + level of indeterminacy (I) + Degree of false (F) < 1.

Contradictory sources of information on a variable, the proposition is:

Degree of truth (T) + level of indeterminacy (I) + Degree of false (F) > 1.

In FBID directly give the results of one type of network into another type of networks. FBID divide the number of zones into two zones, that is region and field, and relational represents are sent from one network to another network. It gives better predicted results based on the previous data. So FBID provide more benefits when compared to existing systems. It's shown in Table 5.1.

6. Experiments and Results. In this simulation evaluating the performance of the FBID protocol using IEEE802.11 standards. Our results are generated based on the FBID protocol. In our simulations, we are concentrate on the Throughput, Packet delivery ratio and energy consumption through the following factors. Ambiguous Collision, Limited Transmission power, False Misbehavior Report, Partial dropping, Receiver collision and collusion all are shown in the Fig. 6.1.

7. Conclusion. Mobile adhoc network is an autonomous collection of nodes. Nodes are changed the position randomly or dynamically throughout the communication. This infrastructure less environment the hackers are easily entered and access the network. These issues are solved by the following methodologies and protocols ACK, S-ACK, AACK, EAACK, AODV, DSR and DSDV etc. But these methodologies still they are suffer to improve the system performance. The proposed fuzzy based intrusion detection protocol, it improves the performance of watchdog limitations. It can be measured by number of factors; Throughput, Packet delivery ratio, propagation delay, routing overhead and finding the shortest path. This on demand based fuzzy based intrusion detection protocol; it improves the performance and doesn't degrade the networking functionalities.

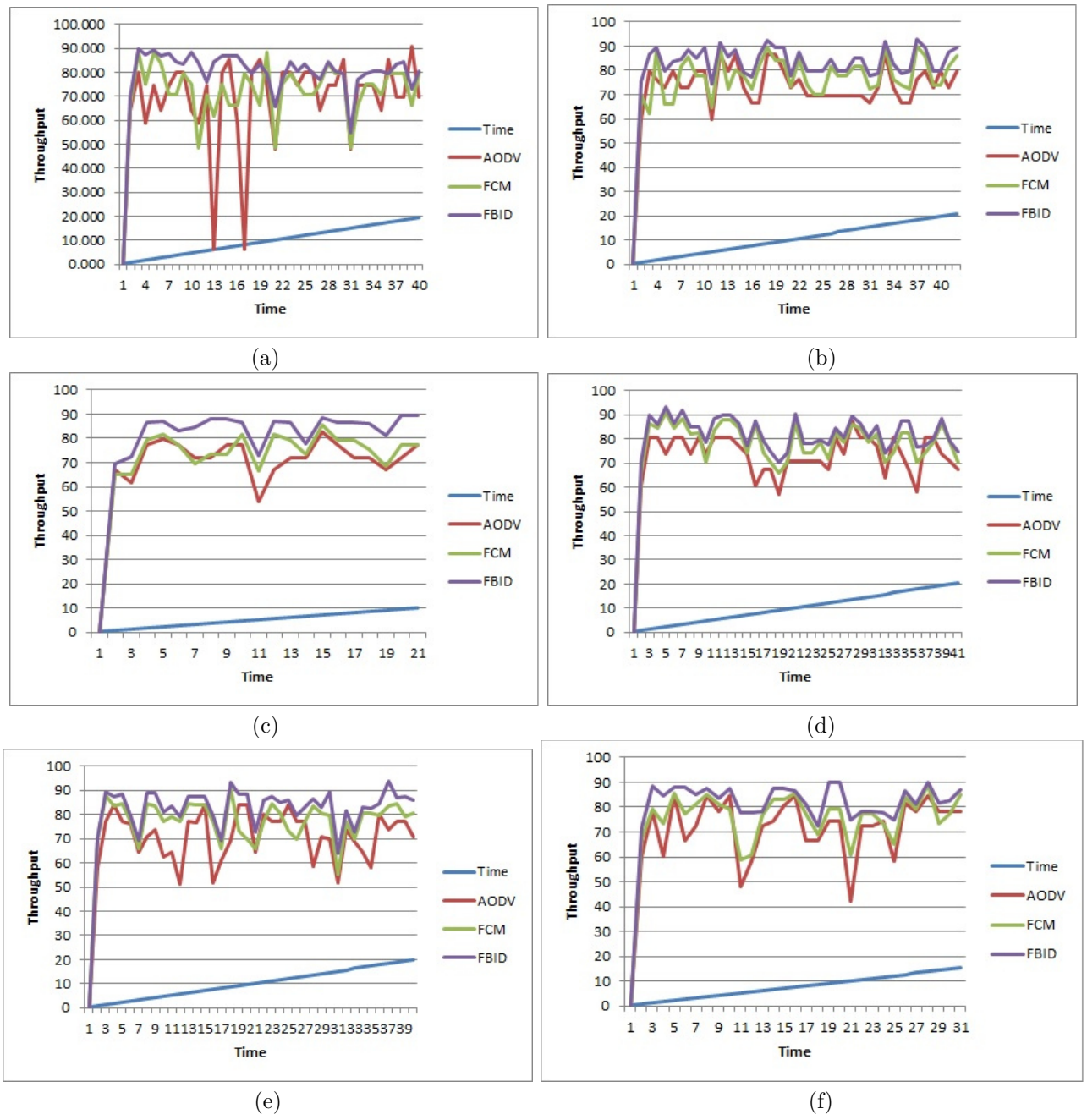

FIG. 6.1. *(a) Ambiguous Collision; (b) Limited Transmission Power; (c) False Misbehavior Report; (d) Partial Dropping; (e) Receiver Collision; (f) Collusion*

REFERENCES

[1] E. M. SHAKSHUKI, N. KANG AND T. R. SHELTAMI, *EAACK - a secure intrusion detection system for MANETs*,IEEE Trans. Ind. Electron.2013, 1089-1098.

[2] NINGRINLA MARCHANG, RAJA DATTA AND SAJAL K.DAS, *A Novel Approach for efficient Usage of Intrusion Detection System in Mobile Ad hoc Networks*,IEEE Transactions on Vehicular Technology, Vol.66,No.2,pp.1684-1695,2017 .

[3] T.KAVITHA, K.GEETHA, R. MUTHAIAH, *Intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach*,Journal of Medical Systems, 2019.

[4] Gurveen Vaseer, Garima Ghai, Dhruva Ghai, *Novel Intrusion Detection and prevention for Mobile ad hoc networks: A single – and Multiattack case study*,IEEE xplore digital Library, 2019.
[5] Basant Subba, Santhosh Biswas, Sushanta Karmakar, *Intrusion detection in Mobile Ad –hoc Networks: Bayesian game formulation*,Engineering Science and technology, an international journal, 2016 .
[6] Otrok, H., et al., *A game-theoretic intrusion detection model for mobile ad hoc networks*, Elsevier Computer Communications (2008)
[7] H. Syed Siddiq and M. Hymavathi, *EAACK - to overcome from intruders attacks in MANETs by providing security checks*, International Journal of Science and Research (IJSR) 2014, 2105-2111.
[8] C. Manikopoulos and L. Ling, *Architecture of the Mobile Ad-hoc Network Security (MANS) system*, in Proc. IEEE Int. Conf. Syst., Man Cybern., Oct. 2003, vol. 4, pp. 3122–3127.
[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang., *Security in mobile ad hoc networks: Challenges and solutions*, Wireless Communications, IEEE, 11 (1): 38–47, 2004.
[10] R. K. Kapur, S. K. Khatri, *Analysis of attacks on routing protocols in ANETs*, Computer Engineering and Applications (ICACEA) 2015 International Conference on Advances in, pp. 791-798, 2015.
[11] K. Nadkarni and A. Mishra, *Intrusion detection in MANETs—The second wall of defense*, in Proc. IEEE Ind. Electron. Soc. Conf., Roanoke, VA, USA, Nov. 2–6, 2003, pp. 1235–1239.
[12] A. Saeed, A. Raza and H. Abbas, *A Survey on Network Layer Attacks and AODV Defense in Mobile Ad Hoc Networks*, Software Security and Reliability-Companion (SERE-C) 2014 IEEE Eighth International Conference on, pp. 185-191, 2014.
[13] D. Djenouri, L. Khelladi, and N. Badache, *A survey of security issues in mobile ad hoc networks*, IEEE communications surveys, 2005
[14] M. S. Khan, Q. K. Jadoon, M. I. Khan, *A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks*, in Mobile and Wireless Technology 2015, Springer Berlin Heidelberg, pp. 137-145, 2015.
[15] C. Siva Ram Murthy and B.S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2004.
[16] Hamza Aldabbas, Tariq Alwadan, Helge Janicke and Ali AlBayatt, *Data Confidentiality in Mobile Ad hoc Networks*, International Journal of Wireless and Mobile Networks (IJWMN) Vol. 4, No. 1,2012
[17] D.Rajalakshmi,K.Meena, *A Novel based fuzzy cognitive maps protocol for intrusion discovery in Manets*, International journal of recent technology and engineering, Vol.7, 2019.
[18] P. Rajakumar, V. T. Prasanna, A. Pitchaikkannu, *Security attacks and detection schemes in MANET*, Electronics and Communication Systems (ICECS) 2014 International Conference on, pp. 1-6, 2014.
[19] Panos, Ch, Xenakis, Ch and Stavrakakis, I.S , *A novel intrusion detection system for MANETS*, International Conference on Security and Cryptography, 2010.

Edited by: Swaminathan JN
Received: Nov 27, 2019
Accepted: Jan 20, 2020