International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 2, March-April 2019, pp. 322-332. Article ID: IJARET_10_02_031
Available online at http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

AN INTRUSION DETECTION AND AVOIDANCE MECHANISM TO SECURE MANETS

Syeda Kausar Fatima
Research Scholar JNTUH, Prof., DCET, Hyderabad,
Principal NSAKCET, Prof., ECE Dept, JNTUH, India

Dr. Syeda Gauhar Fatima
Research Scholar JNTUH, Prof., DCET, Hyderabad,
Principal NSAKCET, Prof., ECE Dept, JNTUH, India

Dr. Syed Abdul Sattar
Research Scholar JNTUH, Prof., DCET, Hyderabad,
Principal NSAKCET, Prof., ECE Dept, JNTUH, India

Dr. Anita Sheela
Research Scholar JNTUH, Prof., DCET, Hyderabad,
Principal NSAKCET, Prof., ECE Dept, JNTUH, India

ABSTRACT

Maximum of research study in securing mobile adhoc networks (MANETs) has motivated on suggestions which detect and inhibit a particular kind of attack such as sleep deprivation, blackhole, greyhole and rushing attacks. In this paper we propose a generalized intrusion detection and avoidance mechanism. We use an arrangement of anomaly based and knowledge-based intrusion detection. This methodology not only secures MANET from an extensive range of routing assaults but also has the proficiency to detect new unexpected attacks. Simulation outcomes of a case study show that our suggested mechanism can successfully distinguish a variety of attacks, comprising multiple concurrent dissimilar attacks, detect and separate the intruders with an reasonable network overhead

Keywords: Adhoc network security; intrusion detection secure routing

Cite this Article: Syeda Kausar Fatima**,** Dr. Syeda Gauhar Fatima Dr. Syed Abdul Sattar and Dr. Anita Sheela, An Intrusion Detection and Avoidance Mechanism to Secure Manets, *International Journal of Advanced Research in Engineering and Technology*, 10(2), 2019, pp. 322-332.
http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2

1. INTRODUCTION

Mobile adhoc networks (MANETs) routing protocols, such as AODV and DSR, function on the notion that there is no mischievous intruder node in the network. Attacker nodes cause severe interruption without violating the routing protocol over an extensive variety of assaults. Intrusion detection and prevention (IDP) offers a way to safeguard nodes contrary to routing attacks. There are two ID techniques: knowledge-based intrusion detection (KBID) and anomaly-based intrusion detection (ABID). KBID has a possibly little false detection rate but it can only detect attacks whose signatures are in the database. On the other hand, ABID not only offers initial warnings of possible intrusions but also might detect efforts to exploit new and unforeseen susceptibilities; though it is more likely to generate false positives than KBID. In [1] authors proposed Adaptive Intrusion Detection and Prevention (AIDP), which used ABID to detect denial of service (DoS) attacks. This paper is extending to a Generalized Intrusion Detection & Prevention (GIDP) mechanism. We suggest an arrangement of anomaly-based and techniques. GIDP not only safeguards MANETs contrary to a wide variety of attacks but also has the competence to detect new attacks or disturbing actions that reduce network performance; to the best of our understanding this is novel.

The remainder of this paper is systematized as follows. Section II defines the related research to secure MANETs. Section III assesses typical MANETs routing attacks. Section IV presents proposed mechanism, GIDP. Section V demonstrates the implementation of suggested mechanism through a case study, as well as simulation. Lastly, we summarize our results and future work in Section VI.

2. RELATED RESEARCH

Research in securing MANETs has to date frequently committed on detecting and preventing particular attacks. For instance, TOGBAD was suggested in [2] to recognize nodes that challenge to produce blackhole attacks in MANETs that use the OLSR routing protocol.

Kurosawa and Jamalipour [3] propose a blackhole recognition mechanism, this time for AODV. Xiaopeng and Wei [4] recommended a greyhole attack detection pattern for the DSR routing protocol. Ping and Zhang [5] well-thought-out a route request (RREQ) flooding attack in MANETs. They anticipated a RREQ flooding inhibition mechanism established on neighbour's organization. In [6] Perrig and Johnson studied how attackers can take off a rushing attack (RU) in DSR and proposed a rushing attack prevention scheme for MANETs.

However, most scientists have focused on defending MANETs against specific types of attack, some have recommended a more common approach. For example, ARAN [7] is a hop-by-hop genuine routing mechanism that can safeguard MANETs against a number of assaults from outside malicious nodes. A related approach, Ariadne [8] has been proposed for end-to-end authentication established on shared key pairs. We consider more effort is required on mechanisms which can safeguard MANETs against an extensive range of attacks. Its behaviour and actions that outcomes in severe assaults are described below in section III.

3. AODV ROUTING ATTACKS

The on-demand routing protocols in MANETs, such as AODV and DSR, permit impostors to takeoff a broader variety of attacks. In order to demonstrate these routing attacks, we consider AODV in this paper. With AODV we give models of how dissimilar intrusive actions can cause numerous attacks in MANETs.

a) Sleep Deprivation through malicious RREQ

Flooding

Sleep deprivation (SD) [9] is a DoS attack in which an attacker cooperates with the node in a way that looks to be legitimate; but where the purpose of interaction is to keep the victim node out of its power conserving sleep mode. An intruder can cause SD of a node by exploiting the vulnerability of the route discovery process of protocol through malicious route request (RREQ) flooding in the following ways: Malicious RREQ Flooding 1: an intruder broadcasts a RREQ with a destination IP address that is within the network address range, but which does not exist. This will compel all nodes to forward this RREQ because no-one will have the route for this destination IP address. Malicious RREQ Flooding 2: after broadcasting a RREQ an intruder does not wait for the ring traversal time and continues resending the RREQ for the same destination with higher TTL values.

b) Black & Grey Hole by false RREP& packet

Dropping

In AODV, the destination sequence number (dest_seq) is used to describe the freshness of the route. A higher value of dest_seq means a fresher route. On receiving a RREQ an intruder can advertise itself as having the fresh route by sending a Route Reply (RREP) packet with a new dest_seq number larger than the current dest_seq number. In this way the intruder becomes part of the route to that destination. The intruder can then choose to drop all packets, causing a blackhole [3] in the network. The severity of the attack depends on the number of routes in the network the intruder successfully becomes part of; we analyze this further in section V. Greyhole is a special case of blackhole attack, in which intruder simply drops packets selectively, from particular nodes.

c) Rushing attack through a forged RREQ

In order to limit the control packet overhead an on-demand protocol merely needs nodes to forward the first RREQ that reaches for every route discovery. An attacker can exploit by scattering RREQ packets rapidly all over the network so as to destroy any later valid RREQ packets. An intruder can forward the fake rushed RREQ, giving them a higher source sequence (src_seq) number and minimum delay. This will destroy the later legitimate RREQ and increase the possibility of routes that include the intruder will be revealed rather than other valid routes, producing a rushing attack.

4. PROPOSED SCHEME

A. Assumptions

We use ABID to detect intrusion in the network; this requires traffic traces that contain only normal activities to build a training profile. However, in contrast with fixed networks, data resources such as [10] that reflect normal activities or events are not currently available for MANETs. Therefore, we assume that the initial behaviour of the network formed on-the fly is free from anomalies. We also disregard attacks aimed at physical and link layer. Further, we have not considered attacks from colluding intruders in this paper. To illustrate the implementation of GIDP we assume a clustered MANET organization. We select the most capable nodes in terms of their processing abilities as cluster heads (CHs) and the other nodes becomes cluster nodes (CNs). At present we assume secure communication between CH and CNs.

B. GIDP Architecture & Terminology

We now describe our proposed mechanism GIDP. GIDP is a hybrid IDP approach that uses a combination of anomaly-based and knowledge-based ID. The architecture of GIDP is shown in Fig.1. A cluster head first gathers data in the form of two matrices: network characteristic matrix (NCM) and a derived matrix (DM). The NCM contains data related to the network routing protocol; for example, in the case study in this paper, NCM consists of seven parameters:

NCM= {RREQ (route request), RREP (route reply), RERR

(routeerror), TTL (time to live) values, RREQ src_seq,

RREQ dest_seq, RREP dest_seq}

The DM consists of parameters which reflects the network performance and can be derived from NCM parameters. For example, in the case study in this paper DM consists of three parameters:

DM= {CPO (control packet overhead), PDR (data packet delivery ratio), CPD (number of control packet dropped)} Then the cluster head employs two phases: training and testing. Fig.2 shows the time-based operation of GIDP. When the network is established, the CH continuously gathers NCM and DM information and applies the GIDP training module for N time intervals (TI), resulting in initial training profiles (ITPs) of NCM and DM.

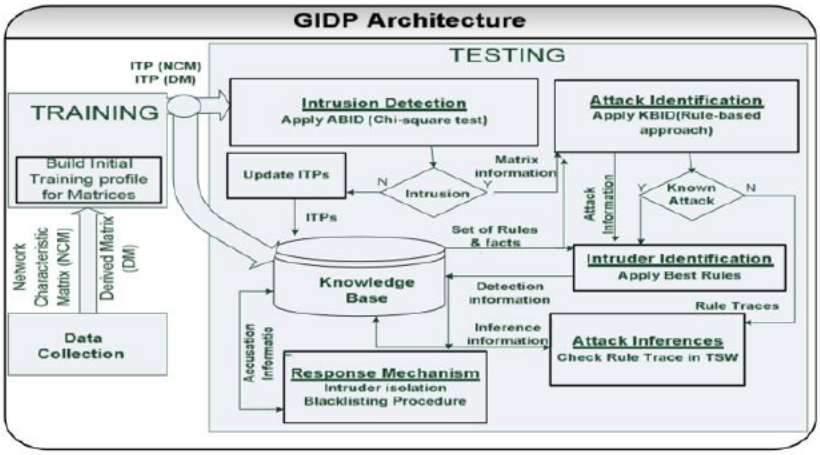

Figure 1 Architecture of GIDP

The ITPs reflects the normal behaviour of the nodes in the network and the expected network performance. In the testing phase the CH applies the testing module after each TI. The testing phase consists of several tasks as shown in fig.1. Firstly, it detects intrusion in the network. If there is no intrusion, then it updates the ITPs in order to adapt the variation in the network behaviour as time progresses. If there is intrusion, in the second task the CH identifies the attack or attacks using existing information in the knowledge base. In the case of known attacks, the CH identifies intruding nodes using intruder identification rules specific to the known attack. To optimise the probability of identifying intruders correctly with a low level of false positives, it maintains a test sliding window (TSW) as shown in fig.2, in which d detections of a node are required in p time intervals (TI). If this detection threshold is passed, then the CH will blacklist the node and isolate the node by informing all CNsIf attack identification detects an attack that does not match the rules for a known attack, then the CH applies the attack inferences. The attack inference module stores the rule trace of current TI as Detected Rule Trace and looks for its match in a TSW. If Detected Rule Trace match is found in a TSW then CH confirms the new attack by constructing & adding a rule for the new attack in the set of rules stored in knowledge base.

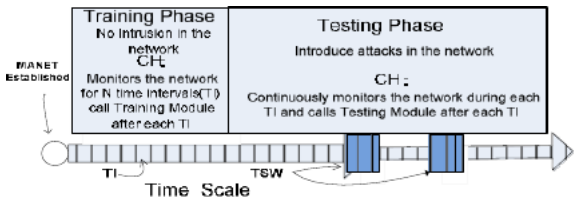

Figure 2 Time-based operation of GIDP.

C. Algorithm & Technical Details

We now explain the GIDP training & testing module.

Training: NCM consists of Xi parameters mentioned above, where i=1 to 7 and each Xi = {X1, X2, X3, XM}is a set of random variables, where M is the maximum number of random variables of parameter Xi. For example, NCM [Xi] represent the number of RREQ received by all CNs in a time interval (TI), where M is the maximum number of RREQ received in a TI. The probability distribution of NCM[Xi] is calculated for the TI. The CH then calculates the DM parameters CPO

(i.e. number of control packet / data packet delivered), PDR (i.e. number of data packet received / data packet originated) & CPD (i.e. number of control packet dropped in establishing & maintaining routes in the network) for the jth TI, and this whole process is then repeated for the N time intervals in the training phase.

We then calculate mean X i of P (NCM [X i]) and means of CPO, PDR and CPD for N intervals, which is then stored as an ITP (NCM) and ITP (DM) respectively containing the expected values for that particular network observed for the total time of N*TI seconds.

Testing: In the testing phase GIDP operates in three stages: a) intrusion detection, b) attack identification and inferences and c) identification and isolation of intruding nodes (Fig.1). Now we explain the algorithms of stage a, b & c. For stage a) it employs ABID using chi-square goodness of fit test on NCM and then KBID using a rule-based approach on both matrices NCM & DM is applied in stage b) and c).

Testing Modules This module only takes NCM parameters into account and applies chi-square test to identify any intrusion in the network.

a. Intrusion Detection

Do after each TI

collect NCM (X i) from all other CNs in TI, for ∀iCalculate the probability distribution P (NCM (X i))

Calculate averages of P (NCM (X i)) & stores as observed values End do

For ∀i Perform Hypothesis Testing by first calculating

Chi- computed ($\chi 2$[i] using eq.1) for Xi

Ho[i]: Observed distribution of NCM (Xi) fits the expected

Ha[i]: Observed distribution of NCM (Xi) does not fit expected If (chi-computed[i] (α.d.f[i]) > P-value[i] (α.d.f[i])) Reject Ho[i]. endif.

End for

. Combined Null Hypothesis Testing

Combine Ho: Observed distribution of NCM fits the expected

Combine Ha: Observed distribution of NCM does not fit expected

. If (combined Ho is rejected)

Perform Attack identification & inferences

else: Update Expected values NCM (X i) (i.e. ITP(NCM))

. Exit

This module continuously monitors the network. In each TI the CH first performs hypothesis testing for each parameter Xi of NCM at calculated chi-computed values obtain from eq.1, where Xi is the parameter of NCM and k (1 to M) is the number of random variables in each parameter Xi. The CH then performs combined hypothesis testing of NCM. If the combined Ho is rejected, then it assumes intrusion in the TI. Else we update the ITP (NCM) using an exponentially weighted moving average (EWMA) and NCM represents the expected and observed value for update period number(q) respectively. The value of q is incremented in the TI when no intrusion in the MANET is detected. k represents the random variable from 1 to M in each Xi and $\alpha=2/(q-1)$ is the weighting factor. As q increases the weighting for older data points decreases exponentially giving more importance to the current observation.

b. Attack identification and inferences

Set up the Interpreter for Rule-based approach

Interpreter applies Forward-Chaining on set of rules Fig.3b (1) If (Any Goal Condition of known attacks are fulfilled) Apply rules for IntruderIdentification & Isolation Fig.3c

endif.

If (Goal Condition==" POTENTIALUNKNOWNATTACK")

Apply Attack Inferences

endif.

Exit.

module. Set of Rules example

Rule.1 ∃x (chi-squaretest (NCM[x]))-> (CheckDerivedMatrix=TRUE)

Rule.2 CheckDerivedMatrix Λ ∃y (Test (DM[y]))->

(PotentialAttack=TRUE) Rule.3 PotentialAttack ->(BestRule=TRUE) Best Rules for some known attacks:

Rule.4 BestRules Λ (chi-squaretest (NCM[RREQ])) Λ

Test (DM[CPO]) -> "SLEEP DEPRIVATION"

Rule.5 BestRules Λ (chi-squaretest (NCM[RREPdest_seq])) Λ

(Test (DM[PDR]) V Lowest (PDR)) -> "BLACKHOLE"

Rule.6 BestRules Λ (chi-squaretest (NCM[RREPdest_seq])) Λ

(Test (DM[PDR]) -> "GREYHOLE"

Rule.7 BestRules Λ (chi-squaretest(NCM[RREQsrc_seq])) Λ

(Test (DM[CPD]) -> "RUSHING"

Rule.8 ¬ (∀x (chi-square-test (NCM[x]))) Λ ¬ (∀y (Test (DM[y]))) -->

"POTENTIALFALSEALARM"

Rule.9 (Rule.1 Λ Rule.2 Λ ¬BestRule) ->

POTENTIALUNKOWNATTACK"

Attack Inferences

If (Detected Rule Trace is Empty)

Store Detected Rule Trace = Rule Trace

Else If (Rule Trace == Detected Rule Trace)

New attack Rule Trace= Rule Trace

Construct a rule for New attack Rule Trace

Append New attack Rule Trace in set of rule trace

Set Detected Rule Trace =Empty. endif

. endif

In case of intrusion the CH calls the Attack Identification and Inferences module. This module obtains a set of rules from the knowledge base. We have constructed these rules from

previous work [1] (i.e. AIDP simulation results), analyzing various attacks & their impact on network performance through

c. Intruder Identification &Isolation

Identifying intruding nodes

a. . Obtain known attack Rules for intruder Identification
b. . for all Goal condition fulfilled
c. Apply intruder identification rule for each detected known attack
    a. add each detected node Vi to List of Nodes Detected (LND)
d. . endfor

Response Mechanism

e. For all nodes Vi in LND
    a. . If (Vi detections in Potential Intruder List (PIL) >
        a. Detections_required_To_ Accuse (d))
    b. CH: Blacklist Vi & Broadcast Accusation Packet (AP) else: enter Vi in PIL endif
f. . End for

Accusation Packet (AP) Handling

g. . Each CN Vi maintain its local BlacklistTable (BLT)
h. . if CN Vi receives an AP for CN Vj
    a. . If CN Vi has node Vj in its BLT then Ignore AP
    b. else: CN adds node Vj to its BLT & rebroadcast AP
    c. . endif
i. . endif

Isolating Intruding Nodes

j. . if node Vi receives packet from node Vj
    a. . If node Vj is in node Vi BLT
    b. Ignore packet & drop all packets queued from Vj
    c. Else: handle & process packet. endif
k. . endif

simulations and analysis of existing literature of known attacks for example [3, 4 & 6]. chi-square test (NCM[x]) predicate returns true if the parameter x is anomalous in NCM. Similarly, predicate or propositional function Test (DM[y]) returns true if the test on parameter y of DM fails. This test uses a tool of Statistical Process Control known as variable control chart based on standard deviation σ. In the Attack Identification & Inference module a ruled base approach is used in which an interpreter can either employ forward or backward chaining system. A forward chaining system process rules one by one by checking premise (condition in the rule) to reach conclusions, it can also draw new conclusions. On the other hand, backward chaining is goal driven, that is it reaches the conclusion first and keeps looking for rules that would allow the conclusion. In GIDP an interpreter applies forward chaining on the set of rules looking for when the Goal Condition is fulfilled. In case of any known attack being detected in the

TI, the interpreter applies the Intruder Identification & Isolation module to identify and isolate the intruding nodes. This module first identifies the intruding nodes by applying known attack rules for intruder identification. For example, in case of a SD attack it employs control chart (explained above) based on σ of RREQ generated by all nodes and adds the detected node

Vi to the LND. Response mechanism (fig.3c(b)) then checks if detection threshold d is reached for any node Vi in the LND in p TI; if so, it blacklists the node Vi and informs all other CNs by sending an AP. When a CN receives an AP it first checks the broadcast id & source address to avoid processing a duplicate AP. If the accused node is already blacklisted the CN will ignore & drop the AP to prevent unnecessary network traffic. Otherwise, the CN will blacklist the accused node and rebroadcast the AP. Finally, to isolate the intruder from the network all nodes will not only drop the packets from a blacklisted node but also immediately ignore all packets in their cue from the blacklisted nodes.

If Goal Condition with POTENTIALUNKNOWNATTACK is fulfilled during the attack identification process, then interpreter save this Rule Trace and looks for the match of this Rule Trace in current TSW. If a match is found, then it confirms new attack detection by constructing a new rule and appending the new rule in a Set of Rule stored in knowledge base.

5. CASE STUDY AND EVALUATION

To assess the applicability and performance of GIDP, we considered a case study with different attack scenarios. We present the simulation results of these scenarios and some key findings from the analysis of attacks. We used GloMoSim to build the simulation environment and then evaluate GIDP using simulation & GIDP parameters shown in Table 1.

Table 1 Simulation & GIDP Parameters

Simulation Parameters		
Number of nodes	25	50
Terrain dimensions	500*500 metres	707 *707 metres
Node placement	Uniform distribution	
Simulation Traffic	CBR (Constant Bit Rate)	
Simulation time	2500 seconds	
Routing protocol	AODV	
MAC protocol	IEEE 802.11	
Mobility	Random Way Point Model (RWP)	
GIDP Parameters		
Time interval TI	100 seconds	
Training, Testing TI	Training=5 TIs, Testing= 20 TIs	
Number of parameters	NCM =7 & DM=3 parameters	
Chi-square test (α)	5% (i.e. 95% confidence interval)	
Test Sliding Window (TSW)	5 TIs	
Detections-Required To_Accuse (*d*)	2 in a TSW	
Number of intruders	Varies 1to 4	

A. Scenario 1

In the first scenario we test GIDP with a denial of service attack (sleep deprivation) through malicious RREQ flooding (MRF), as described in section III-a. The intruders launch MRF1 or MRF2 attacks. At each tested mean speed and for each network size (25 or 50 nodes) we performed 40 runs with no intrusion and 40 runs with intruders using a mix of both MRF1 and MRF 2.

The graph on the left in Fig. 3 depicts the success rate (SR) and false alarm (FA) rate of GIDP as a function of the nodes' mean speed in 25 & 50 node

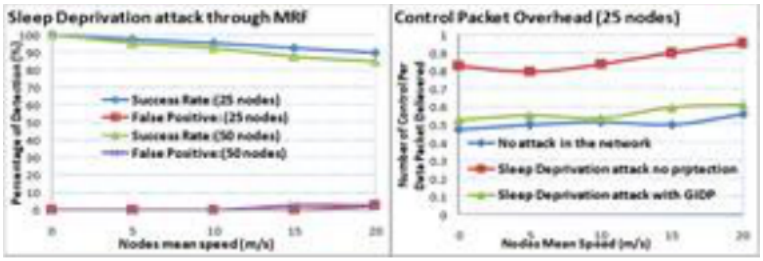

Figure 3 Success rate, false alarm rate and control packet overhead as a function of nodes mean speed (m/s).

networks with SD attack. By SR here we mean the rate of correctly detecting intrusion in the network, identifying the attack type and then identifying & isolating the node which is causing the attack. A false alarm (FA) means that a correctly behaving node has been incorrectly identified and isolated. The graph shows good performance of GIDP in terms of high SR and low FA rates against SD attack. The control packet overhead in a 25-node network when there is a) no attack in the network, b) a sleep deprivation attack with no protection and c) a sleep deprivation attack with GIDP in place. The graph shows that GIDP reduces the control packet overhead and increases network performance when it is used in a network under sleep deprivation attack.

B. Scenario 2

In the second scenario we test GIDP with a mix of black and grey hole attacks caused by initiating a false RREP and then dropping packets as described in section III-b. In order to launch these attacks, on receiving a RREQ an intruder generates a false RREP packet with dest_seq=current dest_seq+f. Through simulations we observed that the value of f should be at least 5 in a 25-node network, and higher for larger networks, because some properly behaving nodes have routes fresher than the intruding node for the destination node. We also note that the severity of the attacks depends on the number of paths in the network that the intruder manages to capture. One false RREP packet only allows an intruder to capture the route of one node in the network, because RREP packets are unicast.

A single simulation consists of 20 test TIs. We monitor the number of false RREP packets (e) generated by an intruding node in a simulation and its impact on packet delivery ratio, increasing the value of e reduces the packet delivery ratio during the BH attack and therefore increases the severity of the attack.

The graph on the left in Fig.4 depicts the SR and FA of GIDP with black & grey hole attack with $8 \leq e < 20$ and $5 \leq f \leq 30$. The graph on the right in Fig.4 shows the packet delivery ratio with no attack, black & grey hole attack with no protection and black & grey hole attacks with GIDP in place. It shows that GIDP can successfully detect these attacks and identify & isolate the intruding node and by doing so GIDP also improves the network performance in terms of packet delivery ratio.

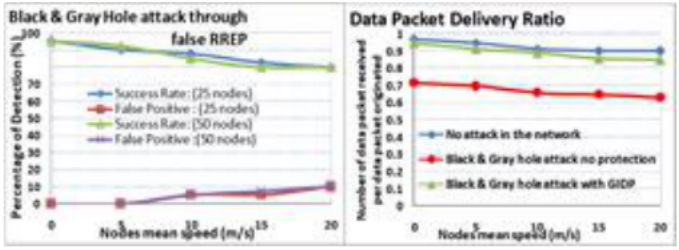

Figure 4 Success rate, false alarm rate and packet delivery ratio as a function of nodes mean speed (m/s).

C. Scenario.3.

In this scenario we tested GIDP with the rushing attack through forged RREQ as explained in section III-

c. We note that intruders trying to cause a rushing attack by sending a forged RREQ with a higher src_seq and minimum delay increase the number of control packets (i.e. RREQ+RREP+RERR) dropped in the network. Fig.5 shows that GIDP can detect rushing attacks and after isolating the intruder reduces the number of control packets dropped.

80

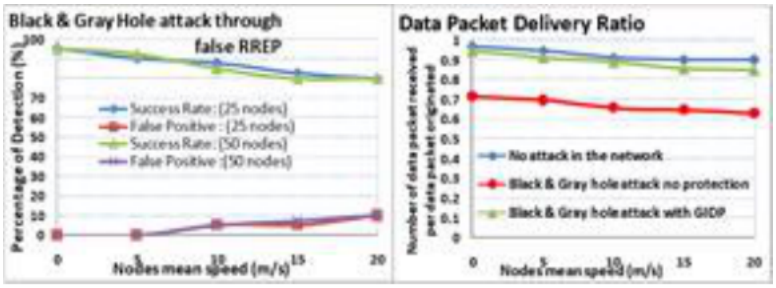

Figure 5 Success rate, false alarm rate and control packet dropped as a function of nodes mean speed (m/s).

D. Scenario 4

In the last scenario we assess GIDP with a combination of simultaneous attacks (section III) launched by separate intruders in a simulation. We perform 20 runs with each combination of attacks. SR here means that GIDP has detected, identified and isolated all the intruders causing attacks. FA means GIDP has detected and isolated a properly behaving node as an intruder.

6. CONCLUSIONS AND FUTURE WORK

Many proposals have been made in the literature to detect various attacks, but most are attack-specific. Unlike some mechanisms that provide protection through authenticated routing, in this paper we have proposed a Generalized Intrusion Detection & Prevention mechanism which monitors both network layer characteristics (NCM) and performance statistics (DM). GIDP uses a combination of anomaly-based and knowledge-based ID that can protect MANETs against a variety of attacks from both external and internal intruders and also has the capability of detecting new unforeseen vulnerabilities. Simulation results show our proposed mechanism can secure MANETs from a wide variety of attacks with an affordable processing overhead. In our ongoing work we are focusing on implementation issues of GIDP and so that it can operate & adapt to networks with different security requirements.

REFERENCES

[1] A.Nadeem and M.Howarth, “Adaptive intrusion detection & prevention of Denial of Service attacks in MANETs”, Proceedings of ACM 5th International Wireless Communication and Mobile Computing Conference, Germany, June 2009.

[2] E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle, “Detecting Black Hole Attack in Tactical MANETs using Topology Graph”, Proceedings of 32nd IEEE Conference on Local Computer Networks, 2007.

[3] S.kurosawa and A.Jamalipour, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, November 2007.

[4] G.Xiaopeng and C.Wei, “A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks”, Proceedings of IFIP International Conference on Network & Parallel Computing, 2007.

[5] P.Yi, Z.Dai and S.Zhang, "Resisting Flooding Attack in Ad Hoc Networks", Proceedings of IEEE Conference on Information Technology: Coding and Computing", Vol.2, pp 657-662, 2005.

[6] Y. Hu, A.Perrig and B.Johnson, "Rushing Attack and Defense in Wireless Ad Hoc Networks Routing Protocols", Proceedings of 2nd ACM workshop on Wireless Security, New York, 2003.

[7] K.Sanzgiri and M.Belding-Royer, "A Secure Routing Protocol for Ad Hoc networks", Proceedings of 10th IEEE International Conference on Network Protocol 2002, (ICNP' 02).

[8] Y. Hu, A.Perrig and B.Johnson, "A Secure On Demand Routing Protocol for Ad Hoc networks", Proceedings of MobiCom, Atlanta, Georgia, USA, pp 23-28, September 2002.

[9] M.Pirrete and R.Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence", International Journal of Distributed Sensor networks, Vol.2, No.3, pp 267-287, 2006.

[10] KDD data set, 1999. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[11] Kusum Nara and Aman Dureja, A Dynamic Approach for Improving Performance of Intrusion Detection System Over Manet, International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 4, pp. 61-81 July-August (2013),

[12] Anirudha A. Kolpyakwar, Sonal Honale, Piyush M. Dhande and Pallavi A. Chaudhari, A Review on Cloud-Based Intrusion Detection System for Android Smartphones, International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 4, Issue 6, pp. 238-245, September – October 2013

[13] Dr Syeda Gauhar Fatima, Syeda Kausar Fatima, Dr Syed Abdul Sattar and Syed Adil, A Study on Intrusion Detection, International Journal of Advanced Research in Engineering and Technology, 10(2), pp. (143-154), 2019

[14] D. Rajalakshmi and Dr. K. Meena, A Survey of Intrusion Detection with Higher Malicious Misbehavior Detection in MANET, International Journal of Civil Engineering and Technology, 8(10), pp. 99–110,2017

[15] V. Jaiganesh and Dr. P. Sumathi, An Efficient Intrusion Detection Using Relevance Vector Machine, International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 1, pp. 383-391, January- February 2013

[16] Sajani J and Dr. S. Manikandan, Analysing and Monitoring of Network IDS Using Intrusion Detection. International Journal of Computer Engineering & Technology, 8(3), pp. 20–27, 2017

[17] Bejoy B J and Dr. Janakiraman S, Artificial Immune System Based Intrusion Detection Systems- A Comprehensive Review. International Journal of Computer Engineering & Technology, 8(1), pp. 85–95, 2017

[18] Syeda Gauhar Fatima, Dr. Syed Abdul Sattar and Dr.K.Anita Sheela, Energy Efficient Intrusion Detection System for WSN, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 3, pp. 246-250, October- December (2012)

[19] Jyoti Attri and Suman Kumari, Enhanced Power-Aware Hybrid Intrusion Detection Architecture in an Ad-Hoc Network Using Mobile Agents, International Journal of Computer Engineering and Technology (IJCET), Volume 5, Issue 7, pp. 85-92, July 2014.