www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Vol.8, Issue.3, June 2020
Research Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

A Secured Data against Attacks in Intrusion Detection System with Dynamic Source Routing Protocol Using Counter Measure Selection Algorithm

A. Muruganandam[1*], M. Natarajan[2], M. Thirunavukkarasu[3]

[1]Dept. of Computer Science, Don Bosco College, Periyar University, Salem, TamilNadu
[2]Dept. of Computer Science, Thanthai Hans Roever College (Autonomous), Bharathidasan University, Trichy, TamilNadu
[3]Dept. of Computer Science, Mahendra Arts & Science College (Autonomous), Periyar University, Salem, TamilNadu

[*]*Corresponding Author: murugandbc1976@gmail.com, Tel.: +91-9842636119*

Received: 25/Apr/2020, Accepted: 13/May/2020, Published: 30/June/2020

Abstract— In this work has been executed the Intrusion Detection System (IDS) technique dependent on the rule of system, hub, or data misuse location framework that can precisely think about the marks of known assaults and has a low pace of support disappointment alerts. Security is a significant worry in remote innovation, and this street numbers security in the remote portable Adhoc organize by utilizing Novel IDS in the Dynamic Source Routing (DSR) directing convention. We control remote versatile specially appointed system hubs to get refreshes from obscure or undesirable hubs in a similar system by means of directing table. We utilize a novel interruption recognition procedure utilizing steering conventions in MANET. It is a famous, productive, straightforward and secure method for imparting between at least two versatile clients, and we can securely send information, data, updates, and signals starting with one end then onto the next utilizing Novel IDS innovation and by hindering of obscure hubs in MANET. In this investigation work created by utilizing the reproduction device NS2 for playing out our strategy.

Keywords— EAIDC, Counter Measure Selection, DSR, IDS, MANET.

I. INTRODUCTION

MANETs have bound unmistakable qualities that assemble them defenseless to numerous styles of assaults. Since they are conveyed partner in nursing open environmental factors any place all hubs co-work in sending the bundles inside the system, malignant hubs are inconvenient to take note. Henceforth it's very inconvenient to style a safe convention contrasted with wired or framework based remote systems. This segment talks about some of the issues and difficulties that an originator of secure conventions faces. These issues are examined as to the principal objectives of a protected convention – classification, uprightness and handiness, believability and non-renouncement. The assaults and dangers permitted by existing Eduard MANET directing conventions are then referenced. The working of some safe directing conventions that address these dangers like SEAD, ARIADNE, ARAN and SRP is then outlining. Back to back segment talks about another essential issue in MANET declaration based validation. It reviews a few instruments arranged and investigates the necessities for compelling endorsement based verification in MANETs.

A. objectives

- Another Intrusion Detection System called Enhanced Adaptive Intrusion Detection and Countermeasure determination (EAIDC) with Dynamic Source Routing (DSR) Protocol explicitly produced for MANETs.
- Compared to contemporary approaches, EAIDC, under certain circumstances, show higher levels of malfunctions, while network performance does not significantly affect them.
- EAIDC can identify vindictive hubs regardless of the presence of bogus bad conduct and contrast them and other famous components in various situations through recreation.
- EAIDC may show higher detection rates for malicious behavior in certain circumstances, while network performance will not be significant.

II. LITERATURE SURVEY

This segment speaks to the review of related paper dependent on the ebb and flows investigate. These papers are not totally identified with the proposed approach however certainly upgrade the presentation of system. NICE (Network Intrusion Detection and Countermeasure Selection), another multi-stage circulated organize interruption location and counteraction structure in a virtual systems administration condition. Decent catches and reviews dubious virtual system framework traffic without intruding on clients' applications and virtual system framework administrations. Through programmable system draws near, NICE can improve the

assault identification likelihood and improve the strength to VM abuse assault without hindering existing ordinary virtual system framework administrations. Pleasant utilizes a novel assault diagram approach for assault location and anticipation by connecting assault conduct and furthermore proposes successful countermeasures. Decent streamlines the usage on virtual system framework servers to limit asset utilization [1]. Versatile impromptu system is enduring with different assaults because of the foundation less system. Thus, MANET needs quite certain security techniques to identify bogus passage of the trouble making hubs. The systems function admirably if the hubs are trusty and act properly helpfully. In this paper, we are distinguishing and identifying bundle dropping hubs utilizing Support vector machine. Bolster vector machine is utilized responsively to group hubs in two unique classes either ordinary or malevolent hubs. SVM takes as info the neighbor trust esteem, determined with information bundles and control parcels. Our strategy is executed with AODV (Ad-hoc on request vector steering) convention. Our test results assessed utilizing parcel conveyance proportion (PDR), End-To-End delay, Average throughput, Normalized Routing Overhead, Average Energy Consumption [2]. We present another circulated directing convention for versatile, multihop, remote systems. The convention is one of a group of conventions which we term "connect inversion" calculations. The convention's response is organized as a transiently requested succession of diffusing calculations; every calculation comprising of a grouping of coordinated connection inversions. The convention is exceptionally versatile, proficient and adaptable; being most appropriate for use in enormous, thick, portable systems. In these systems, the convention's response to interface disappointments commonly includes just a limited "single go" of the circulated calculation. This capacity is interesting among conventions which are steady despite arrange parcels, and results in the convention's high level of adaptivity. This alluring conduct is accomplished through the novel utilization of a "physical or sensible clock" to set up the "worldly request" of topological change occasions which is utilized to structure (or request) the calculation's response to topological changes. We allude to the convention as the transiently requested steering calculation (TORA) [3]. Remote Sensor Networks (WSNs) comprise of sensor hubs conveyed in a way to gather data about general condition. Their appropriated nature, multihop information sending, and open remote medium are the elements that make WSNs exceptionally defenseless against security assaults at different levels. Interruption Detection Systems (IDSs) can assume a significant job in identifying and forestalling security assaults. This paper presents momentum Intrusion Detection Systems and some open research issues identified with WSN security [8].

EXISTING SCHEME

In existing strategy we have concentrated on Ad-hoc on request separation vector directing convention and TTL (Time To Leave) calculation, look at the mark of known assaults and has a low pace of parcel dropout's cautions. AODV convention gives unidirectional correspondence. Obscure assaults can't distinguish this current plan.

A. Disadvantages

- Lack of Central Points
- Absence of a Clear Line of Defense and Secure Communication
- Limited Resources
- Mobility

III. PROPOSED SCHEME

MANET is comprises of portable hubs that are operational with a radio transmitter just as a collector which convey legitimately or in a roundabout way with one another by means of bidirectional remote associations. Another Intrusion Detection System called Enhanced Adaptive Intrusion Detection and Countermeasure determination (EAIDC) with Dynamic Source Routing (DSR) Protocol explicitly created for MANETs.

Contrasted with contemporary methodologies, EAIDC, in specific situations, show more elevated levels of breakdowns, while organize execution doesn't essentially influence them. By utilizing Misbehavior Report Authentication (MRA) conspires, EAIDC can identify malignant hubs in spite of the presence of bogus rowdiness and contrast them and other famous components in various situations through recreation. EAIDC may show higher discovery rates for noxious conduct in specific conditions, while organize execution won't be critical.

A. Advantages

- Strong identification and authentication
- Intrusion Detection Systems are not an answer for all security concerns
- Good security strategy
- Human intervention is required.

IV. METHODOLOGY

A. Intrusion Detection Techniques

An interruption is characterized as a progression of activities that bargain the privacy, accessibility, and trustworthiness of a framework. Interruption Detection is a security innovation that attempts to recognize the individuals who are attempting to break a framework without approval and misuse it, and the individuals who have a genuine access to the framework, however misuse their benefits. The framework might be a host PC, a system gadget, a firewall, a switch, a corporate system, or a data framework checked by an interruption location framework.

An IDS progressively screens a framework and the activities of clients in the framework to distinguish interruptions. Since a data framework can experience the ill effects of different sorts of security holes, it is both actually troublesome and expensive to assemble and keep

up a framework that isn't defenseless against assaults. Experience instructs us never to depend on a solitary cautious strategy. An IDS, through the investigation of framework and client tasks, in the quest for undesirable and dubious exercises, can adequately screen and ensure against dangers.

When all is said in done, there are two sorts of interruption recognition: misuse based identification and abnormality based location. An abuse based discovery procedure encodes known assault marks and framework disappointments and stores them in a database. On the off chance that IDS finds a match between current exercises and marks, an alarm is created. Misuse identification strategies are not viable to recognize new assaults because of the absence of fitting marks. An oddity based acknowledgment method makes ordinary profiles of framework states or client conduct and contrasts them and current exercises. On the off chance that a critical deviation is watched, the IDS will raise a caution. Peculiarity location can recognize obscure assaults. Nonetheless, ordinary profiles are typically exceptionally hard to assemble. For instance, in a MANET, the versatility actuated elements make it hard to recognize typicality and peculiarity. It is along these lines increasingly hard to recognize bogus alerts and genuine interruptions. The capacity to set up typical profiles is basic to the structure of an effective, peculiarity based IDS.

As a promising other option, determination based acknowledgment methods consolidate the upsides of abuse discovery and inconsistency recognition using physically created particulars to portray real framework conduct. Particular based recognition approaches are like the irregularity location techniques, perceiving the two assaults as deviations from a typical profile. Notwithstanding, particular put together acknowledgment approaches depend with respect to physically created determinations to dodge the high pace of bogus alerts. Notwithstanding, the impediment is that the advancement of nitty gritty particulars can be tedious.

Interruption identification frameworks expect to distinguish assaults on PC frameworks and systems, or for the most part against data frameworks. Actually, it is hard to give solid data frameworks and keep them in such a sheltered state during their lifetime and use. Now and then heritage or operational imperatives don't take into account the meaning of a totally secure data framework. Accordingly, interruption location frameworks have the undertaking of checking the utilization of such frameworks to recognize any marvel of perilous conditions. They perceive endeavors and dynamic maltreatment by either genuine clients of the data frameworks or by outside gatherings to mishandle their benefits or to misuse wellbeing holes.

An interruption recognition framework acquires data about a data framework to make a determination about the security status of the last mentioned. The point is to recognize security infringement, endeavored infringement or open shortcomings, which can prompt potential infringement. A run of the mill interruption location framework is appeared in Figure 1.

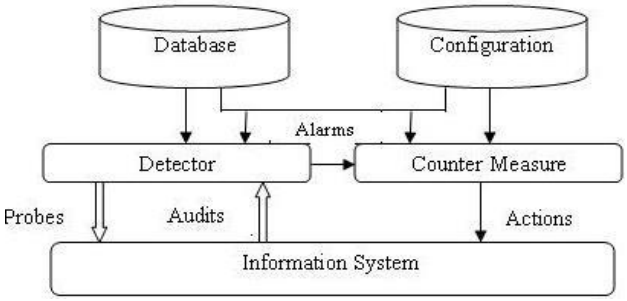

Figure 1. Simple IDS

An interruption location framework can be depicted at an exceptionally plainly visible level as an identifier which forms data from the framework to be ensured (Figure 1). This locator can likewise begin tests to start the review procedure, Such as mentioning rendition numbers for applications. It utilizes three sorts of data: long haul data identified with the procedure used to distinguish interruptions (e.g., an information base of assaults), arrangement data about the present condition of the framework, and review data portraying the occasions that happen framework.

The job of the identifier is to kill superfluous data from the review trail. It at that point presents either an engineered perspective on the security pertinent activities performed during typical utilization of the framework or a manufactured perspective on the present wellbeing state of the framework. A choice is then made to evaluate the probability that these activities or this state might be seen as indications of interruption or shortcomings. A countermeasure part would then be able to take remedial activities to either keep the activities from being performed or to change the condition of the framework to a protected state once more.

B. Implementation of EAIDC Scheme

In this segment we portray our proposed Enhanced Adaptive Intrusion Detection and Countermeasure choice (EAIDC) with Dynamic Source Routing (DSR) Protocol framework in detail. The methodology portrayed in this examination depends on our work to date, where the foundation of EAIDC has been proposed and assessed. In this work, we are growing it with the acquaintance of the advanced mark with keep the aggressor from making receipt bundles.

i. Basic Routing Module

In MANET if the source has no route to the goal, the source starts route disclosure on request. Subsequent to producing RREQ, the hub looks into its own neighbor table to discover in the event that it has a closer neighbor hub to the goal hub. On the off chance that a closer

neighbor is accessible, the RREQ parcel is directed to that hub. On the off chance that there is no more neighbors, the RREQ parcel is overwhelmed to all neighbors.

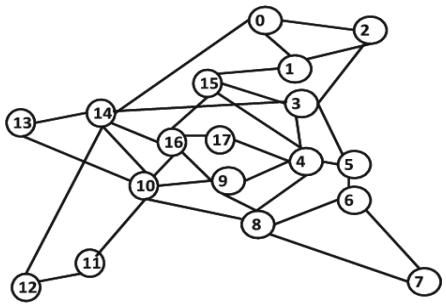

Figure 2. Basic Routing

ii. Secure Acknowledgement

In this module, we actualize a protected affirmation to recognize broken hubs in the steering condition. In this module, we guarantee that the acknowledgment is genuine and not accomplished by Digital Signature.

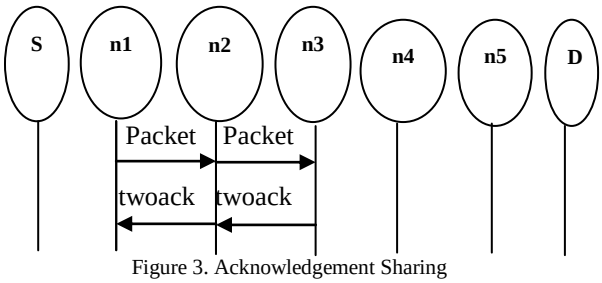

Figure 3. Acknowledgement Sharing

In Figure 3. shows the affirmation sharing at whatever point the source hub S is doesn't get the affirmation, it will begin a protected affirmation process inside three-three hubs. Here, n1, n2, n3 is the first gathering, which hub n1 sends a parcel to hub n2, it will advance it to hub n3 after the two hubs n2 and n1 need to send an affirmation to hub n1 inside time. In the event that the affirmation isn't gotten, it will report these hubs as inadequate hubs to the source hub. In any case, in this procedure there is an opportunity for bogus reports to evade that we execute MRA. Our essential model considering the advanced character creation just by the RSA plot, however in our all-inclusive framework the computerized marking with AES Encryption System made

iii. Misbehavior Report Authentication

In this module, we keep away from bogus reports created by the getting into mischief hubs. The primary objective of the MRA conspire is to confirm whether the objective hub has gotten the announced missing bundle over an alternate course. This technique is utilized in our fundamental model. This plan is intended to understand the shortcoming of bombs hub and to recognize broken hubs with the nearness of a bogus wrongdoing. The bogus unfortunate behavior report can be created by vindictive assailants to report blameless hubs as malignant. This assault can be deadly to the whole system if assailants break enough hubs, causing a system segment. The center of the MRA plot is to validate whether the goal hub has gotten the detailed missing bundle over an alternate course.

To begin the MRA mode, the source hub turns out to be first search for your nearby information base and search for an elective course to the goal hub. In the event that there is no other existing, the source hub begins a DSR steering solicitation to locate an alternate course. Because of the idea of MANETs, it is entirely expected to discover a few courses between two hubs. By tolerating an elective way to the objective hub, we sidestep the jumble correspondent hub. On the off chance that the goal hub gets a MRA parcel, it look through its nearby information base and thinks about when the announced bundle is gotten. On the off chance that it is as of now got, at that point it is sure this is an erroneous maltreatment report and who made this report is set apart as malevolent. In any case the unfortunate behavior report is natural and acknowledged. By tolerating MRA plot, this can recognize threatening hubs notwithstanding the presence of bogus offense report.

Assault analyzer performs ready connection; ascertain seriousness of alarm and countermeasure choice. The ideal countermeasures are chosen from countermeasure pool utilizing the countermeasure determination calculation dependent on Return of Investment (ROI).

ROI [t,cm]= $benefit\ t,cm\ cost\ .cm + intrusiveness\ .cm$

The countermeasure which gives least estimation of ROI is chosen as ideal countermeasure.

Algorithm:

If node has to transfer to destination node
Check the routing table
if route found
    Send the data
    Start counting data
    At beginning of data count set the timer to check the counting
If route not found
    Generate the req as normal on routing protocol
    Broadcast to all neighbor to find destination
if Req received
    Checks req is new
    If not
        Ignore
    If yes
        Updates the reveres routes
        Send node to destination

iv. Counter Measure Selection

In this area, we portray the strategies for choosing countermeasures for a given assault situation. The countermeasure serves to:

- Protect the assurance of the objective VMs from trading off; and
- The assault conduct is with the goal that the activities of the assailant can be recognized.

For better assault location, Countermeasure incorporates assault discovery methods into the interruption counteraction forms. We should take note of that the plan of countermeasure doesn't expect to improve any of the current interruption discovery calculations; truth be told, countermeasure gives just programming system that is reasonable for assault location, fitting countermeasure determination, lastly countermeasure additionally gives security approaches that will help in making sure about the general condition.

Countermeasure used to reconfigure the virtual system based framework and screen, control plane over appropriated programmable virtual changes to altogether improve assault discovery. Countermeasure is a procedure, activity, framework or gadget that can forestall or diminish the impact of dangers to a PC server or system. Countermeasure are chosen by assault analyzer and executed by arrange controller. For instance, if the framework recognizes cradle flood, think about a notice for hub 16 (vAlert = 16), for instance, to check the determination of the framework. After the notice is produced, the combined likelihood of hub 16 becomes 1 since this aggressor has just influenced this hub. It will change in the aggregate probabilities of kid hubs of hub 16. Presently the following stage is to choose countermeasures from the pool of countermeasures CM.

v. Attack Analyzer

The primary elements of countermeasure Systems are completed by the analyzer assaults, including methodology, for example, illustrations assault Construction and redesign, alert connection and determination of countermeasures. The procedure of plan and utilization of Graphics assault situation (SAG) comprises of three stages: gathering data, assault diagram development and potential Exploit direction investigation. With this data, assault courses can be demonstrated utilizing SAG with. The analyzer likewise takes assaults Correlation and investigation tasks alerts. This part has two primary capacities:

- Create Picture Notification Correlation (ACG)
- Provide information about threats and corrective actions to the network controller for virtual networks

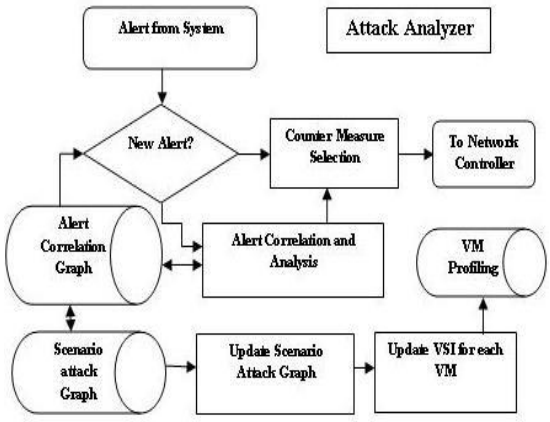

Figure 4 Workflow of Attack Analyzer

Figure 4 shows the work process in the assault examination part. Subsequent to getting a notice from the framework, the alert analyzer compares to the caution in the ACG. In the event that the alert as of now exists in the diagram and is a known assault (i.e., adjusts the assault signature), the assault analyzer plays out a countermeasure determination technique after the framework, and afterward quickly tells the system controller to utilize countermeasures or therapeutic measures. At the point when the admonition is new, the assault analyzer plays out a notice relationship and work process investigation, and updates ACG and SAG. This calculation associates each new admonition with a coordinating ready connection set (i.e., in a similar assault situation). A chose countermeasure is applied by the system controller dependent on the seriousness of the assessment results. On the off chance that the alarm is another blunder and is absent in the assault chart, the assault analyzer includes the assault diagram and afterward recreates it.

False Alarms

A virtual network system with hundreds of nodes will have a huge amount of warnings raised by Snort. Not all of these warnings can leave, and an effective mechanism is needed to check whether such warnings need to be addressed. Because Snort can be programmed to generate notifications via CVE, an approach that matches our work provides when the alarm is actually related to some weaknesses. If so, the existence of this weak spot in SAG means that the warning is rather a real attack. Thus, the false positive rate will be the common probability of the correlated warnings that will not increase the false positive rate in comparison to each individual false positive rate.

In addition, we cannot keep the case from zero-day attack aside, where the vulnerability is detected by the attacker but not detected by vulnerability scanner. In such a case, the warning is considered real because there is no corresponding node in SAG. Thus, current research does not focus on how to reduce the false negative rate. It is important to note that vulnerability scanning scanners are designed to capture the latest vulnerabilities and synchronize with the latest vulnerability database, be able to reduce the chance of zero-day attacks.

Algorithm

Calculation presents how to choose the ideal counter-measure for a given assault situation. Contribution to the calculation is an alarm, assault diagram G, and a pool of countermeasures CM. The calculation begins by choosing the hub vAlert that compares to the alarm produced by a NICE-A. Before choosing the countermeasure, we tally the separation of vAlert to the objective hub. In the event that the separation is more noteworthy than an edge esteem, we don't perform countermeasure determination however update the ACG to monitor alarms in the framework (line 3). For the source hub vAlert, all the reachable hubs (counting the source hub) are collecte d into a setT (line 6).Because the alarm is produced simply after the assailant

has played out the activity, we set the likelihood of vAlert to 1 and ascertain the new probabilities for the entirety of its youngster (downstream) hubs in the set T (lines 7 and 8). Presently, for all t 2 T the pertinent countermeasures in CM are chosen and new probabilities are determined by the adequacy of the chose countermeasures (lines 13 and 14).

The adjustment in likelihood of target hub gives the advantage for the applied counter-measure utilizing (7). In the following twofold for-circle, we process the Return of Investment (ROI) for each advantage of the applied countermeasure dependent on (8). The countermeasure which when applied on a hub gives minimal estimation of ROI, is viewed as the ideal countermeasure. At long last, SAG and ACG are additionally refreshed before ending the calculation. The multifaceted nature of Algorithm 2 is (|V| x |CM|), where |V| is the quantity of vulnerabilities and |CM| speaks to the quantity of countermeasures.

Performance analysis

The system execution alludes to the administration nature of a correspondence item as observed by the client. There are a wide range of approaches to live the exhibition of a system on the grounds that each system is totally unique in nature and style. The outcomes, we finish up, that affirmation based frameworks, including TWOACK, AACK, EAIDC are fit for identifying glitches with the nearness of beneficiary impact and constrained transmit power. In any case, if the quantity of pernicious hubs arrives at 40%, our proposed plot EAIDC execution is lower than that of TWOACK and AACK.

Table 1.1 Routing overhead of Best result in Performance Values of various techniques

Tech. / Scheme	0%	10%	20%	30%	40%
DSR	0.25	0.3	0.35	0.4	0.6
TWO ACK	0.2	0.03	0.3	0.35	0.45
AACK	0.1	0.2	0.25	0.22	0.37
EAIDC	0.001	0.1	0.2	0.21	0.3

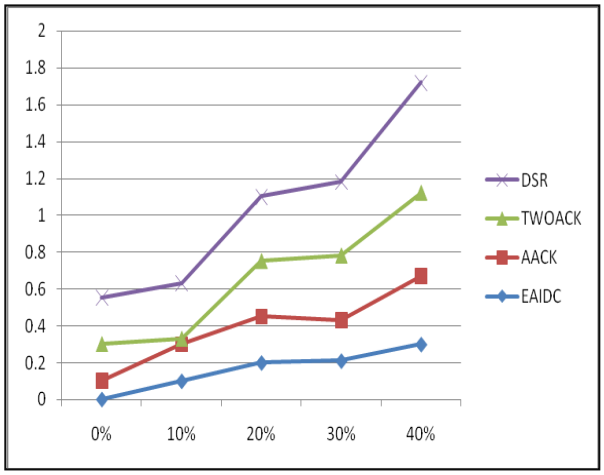

Chart 1.1: Performance Analyse in XGraph

V. RESULT AND DISCUSSION

We used Network test framework 2 (NS2) for execution of proposed work. The methodologies we acclimated are more noteworthy bracing fear change and use computation to strengthen the fulfillment of radio framework. In our exploration work we are utilizing the system recreation instrument for NS2.

Table 6.1 Simulation Parameters

Protocols	DSR
Simulation Time	100s
No. of Nodes	10
Dim. of simulated area	800x600
Speed	30ms
Traffic Type	Constant Bit Rate
Packet Size	1000 bytes
Pause Time	10-100s
No. of Constructions	10
Packet Delivery Ratio	90
Analyzing Rate	85
Throughput	96

We can calculate the following parameters:

1. PDR (Packet Delivery Ratio) - It is the quantity of conveyed information bundle to the hub. More prominent is the estimation of bundle conveyance proportion better is the exhibition of the hub.

PDR= (Number of Packet's Transmitted) / (Total Number of Incoming Packets)

2. CO (Control Overhead) - The proportion of the quantity of steering convention control parcels transmitted to the quantity of information bundles is known as Control overhead.

CO = (Number of Control Packet's Transmitted) / (Total Number of Packets)

3. PMIR (Packet Misroute Rate) - Node sends parcel to an inappropriate goal is called misroute information bundle. PMIR proportion is the quantity of misroute bundle is conveyed to the transmitted parcels.

PMIR= (Number of Packet's Misrouted) / (Total Number of Incoming Packets)

In the underneath screen shows that the correlation chart for Performance of existing and proposed framework.

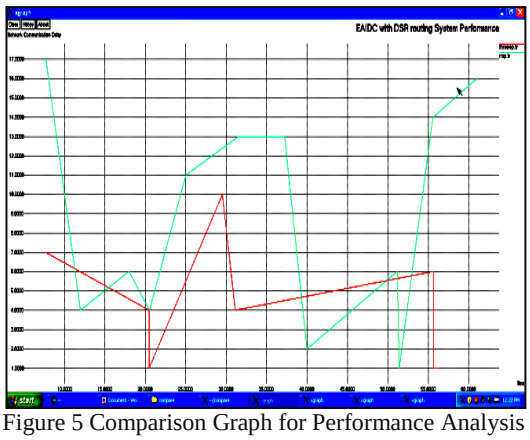

Figure 5 Comparison Graph for Performance Analysis

In the below screen shows that the comparison graph for analyzing rate of existing and proposed system.

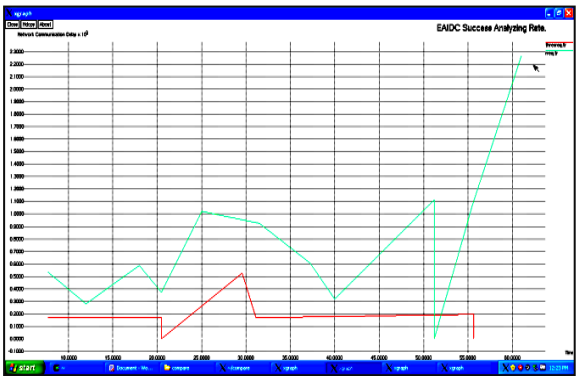

Figure 6 Analyzing Rate

In the below screen shows that the comparison graph for Packet Delivery Ratio (PDR) of existing and proposed system.

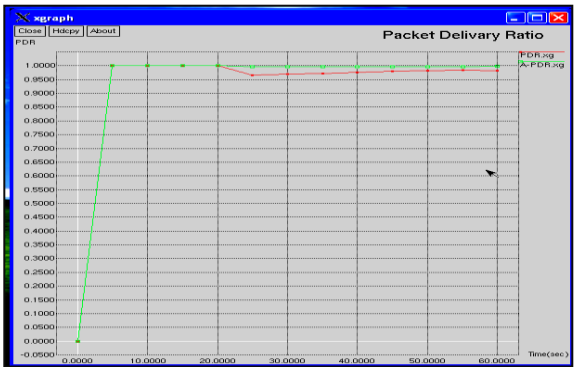

Figure 7 Packet Delivery Ratios

In the below screen shows that the comparison graph for Throughput of existing and proposed system.

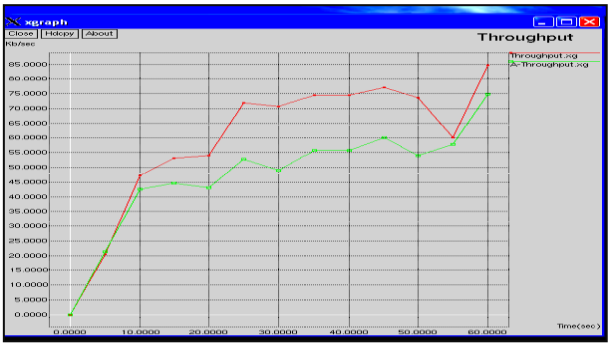

Figure 8 Throughput

VI. CONCLUSION

Package dropping ambush has reliably been a noteworthy risk to security in MANETS. In this assessment, we have proposed novel IDS called EAIDC, which has been unequivocally made for MANETS and differentiated it and other standard instruments in different circumstances through propagations. Besides, we have stretched out our investigation to fuse the propelled mark into our proposed plot with a ultimate objective to shield the aggressors from beginning phony affirmation. As we have showed up in our examination, it can basically improve the PDR of the framework if the aggressors are sufficiently keen to design confirmation packs. We acknowledge that this exchange off is valuable if sort out security is a top need.

FUTURE ENHANCEMENT

So as to expand the benefits of our exploration, we intend to investigate the accompanying themes in our future research:

1) approaches to embrace crossover cryptography strategies to additionally lessen the system trouble brought about by advanced mark;

2) inspect the conceivable outcomes of receiving a key trade instrument to expel the requirement for the recently appropriated keys.

REFERENCES

[1] Prof. Vidya Bodhe, Ms. Megha F. Lingayat “Network Intrusion Detection and Counter Measure Selection in Wireless Sensor Network” ISSN 2321 3361 © 2016 IJESC.

[2] Meenakshi Patel, Sanjay Sharma, Divya Sharan, “Detection and Prevention of Flooding Attack” 2015.

[3] V. D. Park, and M. S. Corson “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks”, Proc. INFOCOM ’97, April 1997.

[4] Alokparna Bandyopadhyay1, Satyanarayana Vuppala2, “A Simulation Analysis of Flooding Attack in MANET usingNS-3” , IEEE 2011.

[5] Meenakshi Patel, Sanjay Sharma, “Detection of Malicious Attack in MANET A Behavioral Approach”, IEEE 2012.

[6] Prasenjit Choudhury, Subrata Nandi, Anita Pal, Narayan .C. Debnath, “Mitigating Route Request Flooding Attack inMANET using Node Reputation”, IEEE 2012.

[7] S.Sanyal, A.Abraham, D.Gada, R.Gorgi, P.Rathore, Z.Dedhia, and N. Moody, “Security scheme for distributed DOS in mobile ad hoc networks”, 6th International Workshop on Distributed Computing (IWDC”040), vol. 3326, LNCS, Springere , 2004 , pp.541.

[8] Nabil Ali Alrajeh, S. Khan, Bilal Shams, “Intrusion Detection Systems in Wireless Sensor Networks: A Review”, 2013, International Journal of Distributed Sensor Networks (Saga Journal) May 2013.

[9] S.Kanan, T.Kaliakikumaran, S. Karthik and V.PArunachalam, “A Review on Attack Prevention Method in MANET” Journal of Modern Mathematics and Statistics Year 2011/Volume :5 /Issues : 1 /Page no. 37-42.

[10] Framework for Intrusion Detection in IEEE 802.11Wireless Mesh Networks, Shafiullah Khan1, 2, Kok-KeongLoo1, and Zia Ud Din3,1School of Engineering and Design, Brunel University, UK.

