IoT: Analysis of Various Attacks Using AODV Protocol

Anbarasi N[1], Prasath Kumar S[2], Mahalakshmi G[1], Duraimurugan J[1], Senthilnayaki B[1]

[1]*Department of Information Science and Technology, Anna University, Chennai, India.*

[2]*Department of ECE, Sri Sai Ram Institute of Technology, India.*

Corresponding Author: anbarasi@auist.net

Abstract: - IoT prompts the vision of associated universe of physical and virtual cycles, administrations and items, which are fit for giving a path on the most proficient method to connect them to web. IoT is a significant piece of future web that essentially coordinates and empowers various correspondence arrangements and innovations and consequently, it is a striking interest to characterize how standard correspondence conventions could uphold the vision of IoT. In this setting, we present a similar investigation on networks dependent on Ad Hoc On-Demand Distance Vector (AODV) network under different assaults like skin hole, dark hole and wormhole.

Key Words: — ***Adhoc networks, ADOV, IOT, Wormhole.***

I. Introduction

At first wired organizations were utilized prominently to interface a PC organization to web however as of late, remote organization have gotten more bountiful in the wide situation. A remote organization permits between availability of heterogeneous frameworks by empowering frameworks to convey and trade data. Further, by the vision of Internet of Things (IoT), an associated universe of virtual and actual gadgets can be interconnected prompting a few chances. However, IoT gives us a few astonishing alternatives yet additionally experiences different weaknesses, for example, An interruption recognition framework (IDS) can be one of the answers for the issue of security in an IoT network. An IDS screens the security condition and make a ready when an interruption conduct is recognized further, the framework executive can make reaction as indicated by the cautions. IDS can decide the contrasts among ordinary and possibly destructive exercises some of them are:

Our Objective in this paper is to present the analysis of an AODV network under various attacks like worm hole, flooding attack and black hole attack. This paper is organized in six sections.

Manuscript revised November 15, 2021; accepted November 16, 2021. Date of publication November 17, 2021.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898; SJIF: 5.494

In section I and II we have discussed the introduction and background of IoT and adhoc networks. In section III we have discussed the implementation details. Further in section IV and V we evaluate and implement our AODV networks. In the last section we have discussed the conclusion and future work.

II. Background

MANETS have become a vital innovation for some IoT application spaces including keen urban areas. It is a self-designing remote organization which is framed having no previous framework. Hubs can move toward any path inside the scope of the arrange and can even go about as a switch. MANETS are mainstream when making of modest, little and amazing organization is thought of and further, its relationship with IoT has expanded its utility to a more significant level. To encourage correspondence in an Adhoc network, a directing convention is required. A steering convention ensures that an effective and a precise course has been set up between various hubs in the organization.

MANET directing conventions are characterized in three significant classifications proactive, responsive and half breed. A responsive steering convention finds a course on request when correspondence between hosts of a versatile organization is needed by flooding the organization with course demand parcels; instances of such conventions are AODV, DSR, and CBR and so on Then again the working of proactive steering conventions is somewhat extraordinary when contrasted with responsive conventions. In proactive conventions course revelations are made consequently and occasionally to develop a table of organization geography model DSDV, OLSR, CGSR and so forth A crossover routing protocol combines the mechanisms of proactive and reactive routing protocols. The initial routing starts with the establishment of some proactively prospected routes and then serve the demand from additionally activated nodes through reactive flooding. The major classification of MANET protocols are given below:

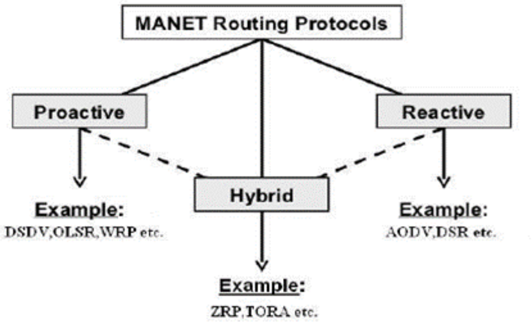


Fig.1. Different Types of MANET protocols

Each directing convention in MANET can experience the ill effects of different assaults in worm opening, dark opening, flooding assault, dim opening assault, narrow minded assault and so on[9]. In this paper we especially center around dark opening assault, flooding assault and worm opening assault. In worm opening assault the assaulting hub catches the bundles from an area and communicates them to another area which further conveys them locally. Then again dark opening assault is a kind of disavowal of-administration assault where a switch that should transfer parcels rather disposes of them. This typically happens from a switch getting traded off from various causes. Further, in flooding assault which additionally a kind of disavowal of-administration assault, which hurts an organization by flooding it with enormous measure of traffic.

III. IMPLEMENTATION

A. Network simulator and trace graph

We have simulated our network in NS2 simulator which is an open source simulation tool designed for Linux. It provides discreet event simulation targeted to network research for wired and wireless network. It also provides support to simulation of multicast protocols, routing and IP protocols like TCP, UDP, and RTP etc. Two key languages of NS2 are C++ and Object-oriented Tool Command Language (OTcl) [10]. The internal mechanism of the simulation objects is defined by C++, on the other hand scheduling discrete events and configuration of the objects is done by OTcl.

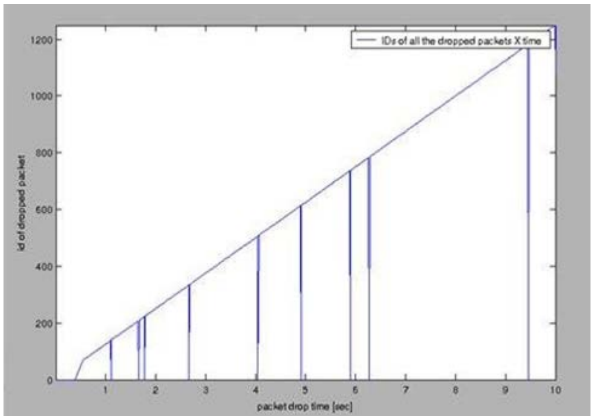


Fig.2. Simulation of flooding attack in AODV

Further, tracegraph is being used to plot the results of the network. Tracegraph allows its users to analyze their network from different ways.

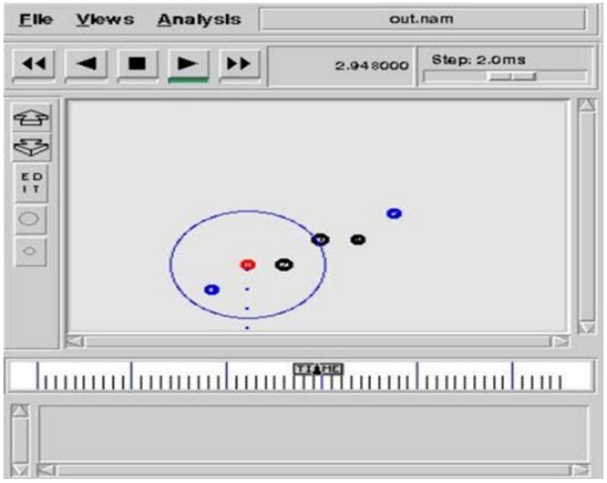


Fig.3. Simulation of flooding attack in AODV

In this section we present the empirical evaluation of our network. In figures 1 the network, which is simulated in NS2, is presented and table 1 shows the basic simulation

The simulation program is written in form of TCL script which is then implemented in NS2 simulator. After the simulation of the network in NS2 two files are generated as result first is the trace file and the second file generated is the network animator file. We have analyzed our network using the trace file. We have used tracegraph to build graphs of the network activities.

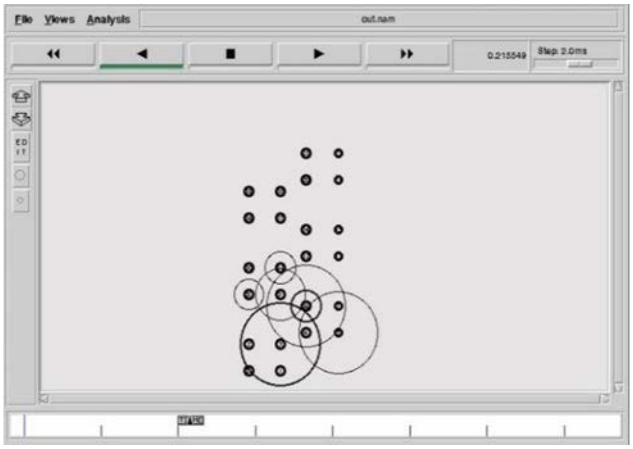
We have also used weka to analyze our trace files. In weka we have used different models like random tree, Naïve Bayes and decision table to analyze our network. information in weka. Once, network has been simulated a trace file is generated which allows us to analyze all activates in our network. We did our experimentation with three different AODV networks simulating worm hole, black hole and flooding attack on the networks and then further analyzing our network by the trace files being generated. Analysis of each network was performed using trace graph which is third party software that helps in making graphs in ns2. Later, weka was used to analyze the trace files generated by each network. Figure 1: Figure.2: Simulation of flooding attack in AODV

In this part, we present the observational appraisal of our association. In figures.2, the association, which is reproduced in NS2, is presented and table 1 shows the major reenactment information in weka. Once, network has been reenacted a follow archive is made which grants us to examine all establishes in our association. We did our experimentation with three assorted AODV networks imitating worm opening, hole opening and flooding attack on the associations

IV. Evaluation

Black hole assault is a sort of Denial of Service assault. During the course revelation noxious hub depicts that it has the best way to the hub objective. On getting a RREQ message it reacts with a phony RREP and further, when the vindictive hub gets parcels from the source it drops the bundles as opposed to sending it. We have reenacted dark opening assault in an AODV network.

Address Probing specialist is a static specialist. It gives benevolent human-PC interface to the customer client. At whatever point a customer is associated with the organization, its location ought to be educated to the worker. These addresses will be helpful to the worker specialist to circulate the screen specialists to all associated customer frameworks.



Worker specialist is a static specialist. It ought to consistently be in the listen mode. It gives amicable human-PC interface to the manager. The worker specialist makes and sends the screen specialist to all the customer hubs at a specific time frame to identify the interruptions in the customer hubs. Interruption endeavors will be educated to the administrator. By investigating this log data, administrator can screen the entire organize and can eliminate doubt customer hubs. Screen Agent is ship off every customer hub for checking. Subsequent to arriving at the customer side, screen specialist makes Forecasting Engine-specialist for expectation. After expectation, the screening specialist will peruse the anticipated records and discover the number of unusual exercises that occurred (or not). Presently it can make two moves: 1. Restorative Action for anomalous movement and 2. Data Action for the ordinary exercises

On the off chance that the screening specialist finds any single movement that is noted as strange, at that point it makes Corrective Agent. Else it makes Information Agent. Both activity specialists are utilized to envision the anticipated records subtleties and Network subtleties. A restorative specialist can eliminate the anomalous movement records from the anticipated documents and furthermore, it sends a report to the manager about the interruption that occurred.

The fundamental method of correspondence between two specialists is through message passing. Very two principle specialists convey legitimately to one another. They are expected to achieve a specific errand. So they should be static after it has been made or dispatched. To impart among customer and worker, primary specialists make communicator specialists to convey.

V. Results And Discussions

The simulation program is written in form of a TCL script which is then implemented in the NS2 simulator. After the simulation of the network in NS2 two files are generated as result first is the trace file and the second file generated is the network animator file. We have analyzed our network using the trace file. We have used tracegraph to build graphs of the network activities. We have also used weka to analyze our association by the follow records being made. Assessment of every association was performed using tracegraph which is untouchable programming that helps in making diagrams in ns2. Subsequently, weka was used to separate the follow records made by every association.

VI. Conclusion And Future Work

IoT security is the area of endeavor concerned with safeguarding connected devices and it has become the need of the hour to take strong steps towards this domain. In this paper we have simulated AODV networks and analyzed the effect of various attacks such as worm hole, black hole and flooding attack on the network. For analysis, we have used WEKA as the data mining tools, which help us retrieving the sent, received and dropped packet information in the networks under attack. For the future work, further level of deep analysis of the network can be done using other attacks.

References

[1]. Shah, S., Khandre, A., Shirole, M., & Bhole, G. (2008, August). Performance evaluation of ad hoc routing protocols using NS2 simulation. In Conf. of Mobile and Pervasive Computing.

[2]. Chen, C., & Ma, J. (2007, May). Simulation study of AODV performance over IEEE 802.15. 4 MAC in WSN with mobile sinks. In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on (Vol. 2, pp. 159-164). IEEE.

[3]. Shakil, K. A., Anis, S., & Alam, M. (2015). Dengue disease prediction using weka data mining tool. arXiv preprint arXiv:1502.05167.

[4]. Abdelshafy, M. A., & King, P. J. (2014). Resisting flooding attacks on AODV. SECURWARE, 25.

[5]. O'Reilly, C., Gluhak, A., Imran, M. A., & Rajasegarar, S. (2014). Anomaly detection in wireless sensor networks in a non-stationary environment. IEEE Communications Surveys & Tutorials, 16(3), 1413-1432.

[6]. Fu, R., Zheng, K., Zhang, D., & Yang, Y. (2011). An intrusion detection scheme based on anomaly mining in Internet of Things.

[7]. Sedjelmaci, H., Senouci, S. M., & Al-Bahri, M. (2016, May). A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. In Communications (ICC), 2016 IEEE International Conference on (pp. 1-6). IEEE.

[8]. Arrington, B., Barnett, L., Rufus, R., & Esterline, A. (2016, August). Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms.

[9]. J.Duraimurugan, N.Anbarai, G.Mahalakshmi & S.Prasath Kumar, “MANET: Efficiency Enhancement Using AZ-Routing Protocol”, International Research Journal of Modernization in Engineering Technology and Sciences, e-ISSN: 2582-5208, Volume: 03/Issue: 09/September-2021.

[10]. G.Mahalakshmi. E.Uma, “Secure Data Transmission in VANET’s Using Efficient Key-Management Techniques”, LNDECT Springer, ICICV 2019.