ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 6, June 2016

An Approach for Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach

Nilesh E. Patil[1], Sagar A. Patil[2], Ravindra B. Raut[3], Vaibhav B. Thorat[4], Prof. Bhagyashree Patle[5]

UG Student, Dept. Of Computer Engineering., SKN Sinhgad Institute of science & Tech., Lonavala, (MS), India[1,2,3,4]
Assistant Professor, Dept. Of Computer Engineering., SKN Sinhgad Institute of science & Tech.Lonavala,`(MS),India [5]

ABSTRACT— In mobile ad hoc networks (MANETs), an essential requirement for the foundation of communication among nodes is that nodes should coordinate with one another. In the presence of malicious nodes, this requirement may lead serious security concerns; for instance, such node may disturb the routing process. In this context, preventing or detecting malicious nodes launching grayhole or collaborative black hole in challenge. This project attempts to determine this issue by designing a dynamic source routing (DSR)- based routing mechanism, which is referred to as the cooperative bait detection scheme(CBDS), that coordinates the advantages of both proactive and reactive defense architectures. Our CBDS system implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing That in the presence of malicious node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics)..

KEYWORDS – Mobile Nodes, Routing, Node discovery.

I. INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs), have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. For detecting the objects, we apply algorithms like SSIM index, Histogram matching [6]. Using Hadoop, we minimize the analysis time. Finally draw the graphs in which show the no of objects to be detected and time to be required for analysis and stored analysis result into database for security purpose.

II. DETAILED DESIGN AND DOCUMENT

INTRODUCTION

This document specifies the design that is used to solve the problem of Product.

ARCHITECTURAL DESIGN

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 6, June 2016

A description of the program architecture is presented. Subsystem design or Block diagram, Package Diagram, Deployment diagram with description is to be presented.

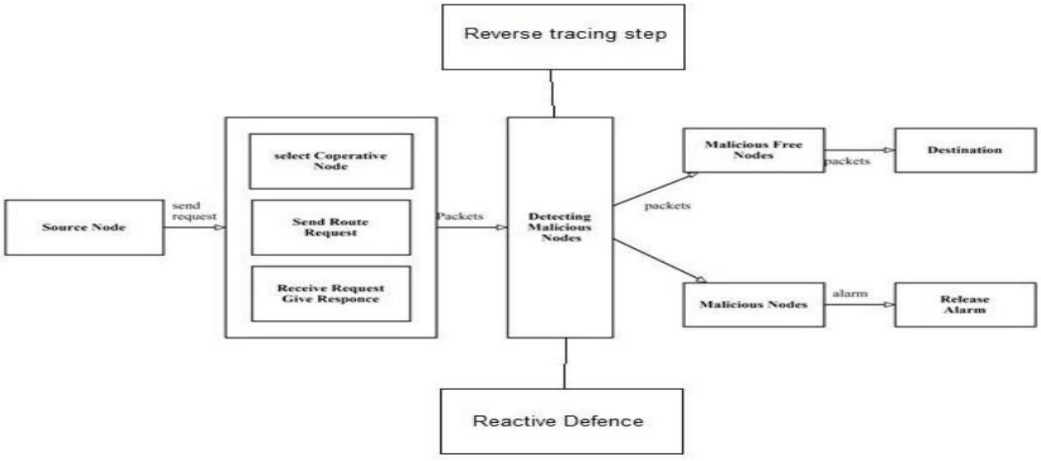

Fig. 1 Architecture diagram

DATA DESIGN (USING APPENDICES A AND B)

A description of all data structures including internal, global, and temporary data structures, database design (tables), file formats. Internal software data structure Data structures that are passed among components the software are described.

Global data structure: Data structured that are available to major portions of the architecture are described.

Temporary data structure: Files created for interim use are described.

Database description: Database(s) / Files created/used as part of the application is(are) described.

OMPOENT DESIGN Class diagrams, Interaction Diagrams, Algorithms. Description of each component description required.

III. PROJECT ANALYSIS OF ALGORITHMIC

DESIGN • To develop the problem under consideration and justify feasibility using concepts of knowledge canvas and IDEA Matrix. Refer [?] for IDEA Matrix and Knowledge canvas model. Case studies are given in this book. IDEA Matrix is represented in the following form. Knowledge canvas represents about identification of opportunity for product. Feasibility is represented w.r.t. business perspective.

Table 1. IDEA Matrix

I	D	E	A
Increase	Drive	Educate	Accelerate
Improve	Deliver	Evaluate	Associate
Ignore	Decrease	Eliminate	Avoid

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 6, June 2016

Project problem statement feasibility assessment using NP-Hard, NP Complete or satisfy ability issues using modern algebra and/or relevant mathematical models.

• Input x, output y, y=f(x)

ALGORITHM

Dynamic Threshold Algorithm

```
01  double threshold=0.9;
02  InitialProactiveDefense( );
03  double Dynamic(threshold)
04  {  double T1, T2;
05        T1=calculate the time of PDR down to threshold;
06        if(PDR < threshold)
07        InitialProactiveDefense( );
08        T2=calculate the time of PDR down to threshold;
09        if(T2 < T1){
10          if(threshold < 0.95)
11          threshold=threshold+0.01;
12        }
13        else{
14            if(threshold > 0.85)
15            threshold=threshold-0.01;
16        }
17        if(SimulationTime < 800){
18        return threshold;
19        Dynamic(threshold);
20        }
21        else
22        return 0.9;
23  }
24
```

IV. PROJECT IMPLEMENTATION

In implementation phase of our project we have implemented various module required of successfully getting expected outcome at the different module levels. With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing. The project takes shape during the implementation phase. This phase involves the construction of the actual project result. Programmers are occupied with encoding, designers are involved in developing graphic material, contractors are building, and the actual reorganisation takes place.

This phase is complete when all of the requirements have been met and when the result corresponds to the design. Modules:

1. Network Model.
2. Initial Bait.
3. Initial Reverse Tracing.
4. Shifted to Reactive Defence Phase.
5. Security Module.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 6, June 2016

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 6, June 2016

V. CONCLUSION

In this approach, we have proposed a new mechanism Cooperative Bait Detection Scheme (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative black hole attacks. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a black hole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. We have observed that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defence architectures to achieve the aforementioned goal. As future work, we intend to 1) investigate the feasibility of adjusting our CBDS approach to address other types of collaborative attacks on MANETs and to 2) investigate the integration of the CBDS with other well-known message security schemes in order to construct a Comprehensive secure routing framework to protect MANETs against miscreants.

REFERENCES

[1] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," J. Mach. Learn. Res., pp. 993–1022, 2003. III. IV.

[2] Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou, "A taxi driving fraud detection system," in Proc. IEEE 11th Int. Conf. Data Mining, 2011, pp. 181–190. V. VI.

[3] D. F. Gleich and L.-h. Lim, "Rank aggregation via nuclear norm minimization," in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 60–68. VII. VIII.

[4] A. Klementiev, D. Roth, K. Small, and I. Titov, "Unsupervised rank aggregation with domain-specific expertise," in Proc. 21st Int. Joint Conf. Artif. Intell., 2009, pp. 1101–1106. IX. X.

[5] A. Klementiev, D. Roth, and K. Small, "Unsupervised rank aggregation with distance-based models," in Proc. 25th Int. Conf. Mach. Learn., 2008, pp. 472–479 XI. XII.

[6] Hengshu Zhu, Hui Xiong, Senior Member, IEEE, Yong Ge, and Enhong Chen, Senior Member, IEEE, "Discovery of Ranking Fraud for Mobile Apps", vol.13,n0.1,Jan 2015 XIII. XIV.

[7] A. Ntoulas, M. Najork, M. Manasse, and D. Fetterly, "Detecting spam web pages through content analysis," in Proc. 15th Int. Conf. World Wide Web, 2006, pp. 83–92. XV. XVI.

[8] N. Spirin and J. Han, "Survey on web spam detection: Principles and algorithms," SIGKDD Explor. Newslett., vol. 13, no. 2, pp. 50– 64, May 2012. XVII. XVIII.

[9] B. Zhou, J. Pei, and Z. Tang, "A spamicity approach to web spam detection," in Proc. SIAM Int. Conf. Data Mining, 2008, pp. 277–288. XIX. XX.

[10] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in Proc. 19thACMInt. Conf. Inform. Knowl. Manage, 2010, pp. 939–948..