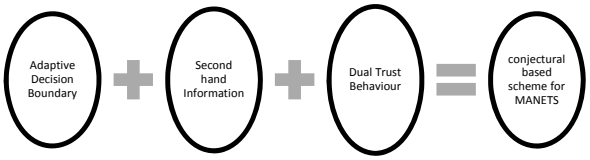
A FRAME WORK OF ADAPTIVE DECISION BOUNDARY, REPUTATION BASED APPROACH AND DUAL TRUST MODEL FOR HANDLING SECURITY ISSUES IN MANETS.

[1]Geetha V, [2]Dr.HariPrasad
[1]Assistant professor, Department of ISE , RVCE, BANGALORE-59 ,
[2]Vice principal & Head, Department of ECE, BMSIT, BANGALORE-64
E-mail: [1]geethavenkatesh21@gmail.com,[2]harivat2002@yahoo.co.in

ABSTRACT

Mobile ad-hoc network is the spontaneous network which has no fixed infrastructure and the topology of the MANETS keeps changing instantaneously. These kinds of networks are prone to changes and adapts to the changes. The effect of misbehaving and malicious nodes in the route discovery process is adverse. The proposed paper gives the solution to the problems created by the malicious nodes and selfish nodes using the reputation based methods and security in the routing mechanism is based on the dual trust scheme. The classification of the selfish nodes and regular nodes is done using the mathematical model called adaptive decision boundary. Our work provides the extent of noncooperation that a network can allow depending on the current strength of nodes for the given scenario and thus includes selfish nodes in network participation with warning messages.



Introduction

For analyzing the security of wireless mobile ad-hoc networks, we need certain parameters [8]. The basic parameters for a secure system are: Authentication Confidentiality, Availability, Integrity, Non-repudiation & Scalability. In mobile ad hoc networks, protecting the network resources from attacks is an important research topic in wireless security. The proposed approach describes a robust and security service scheme for network-layer security solution in ad hoc networks, which preserve both, routing and packet forwarding functionalities without the context of any data forwarding protocol. This approach solves the issue in an efficient manner. The overall idea of this approach is to detect intruder launching attacks and misbehaving links to prevent them from communication network. It is a robust and a very simple idea, which can be implemented and tested in future for more number of attacks, by increasing the number of nodes in the network and routing protocols.

1. Adaptive decision boundary model.

In the ad-hoc network, intruders are compromised or cooperated node, which influence network resources ,degrade network performance and drain battery life of genuine nodes. To detect intruders, an approach advised which maintain record of data packet and RREQ and RREP packet at specific node and Xoring of value of forward and receive of packets and analysis the behavior. If the value of Xoring is 0

then node is recognized as intruders otherwise node is normal.

A. Algorithm

```
Algorithm Int_Node (node,n)
{
DECLARE FWD_packet, RCV_packet
// To keep all possible record for each node in different cases for each neighbor node of selected node
Case1:
 FWD_packet=0 and RCV_packet=0
Case2:
 FWD_packet=1 and RCV_packet=0
 Case3:
 FWD_packet=0 and RCV_packet=1
 Case4:
 FWD_packet=1 and RCV_packet=1
//To check the value of XORing of FWD_packet and RCV_packet to take decisions for malacious
If (FWD_packet XOR RCV_packet==0) then
DISPLAY ―Node is normal‖
ELSE
DISPLAY ―Node is malacious‖
End If
Exit
```

Reputation based scheme

It relies on building a reputation metric for each node according to its behavioral culture. The effective protocol like Dynamic Source Routing Protocol is used. An observing approach used by most systems in this category is called a watchdog. The watchdog was proposed to detect data packet noun forwarding by over-hearing the transmission of the next node. The, entire approach to handle the problem is given in terms of Watchdog mechanism, reputation, second hand information, trust and behavior as follows.

- Observe the action of other nodes – **Watchdog mechanism**
- Develop a perception of other nodes over time – **Reputation**
- Share experiences to facilitate community growth – **Second hand information**
- Predict their future behavior – **Trust**
- Cooperate/Non-cooperate with trustworthy nodes – **Behavior**

3.1 Reputation representation

- **Probabilistic formulation**

Use **beta distribution** to represent reputation of a node.

$$R_{ij} = Beta(\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1} \forall 0 \le x \le 1, \alpha \ge 0, \beta \ge 0$$

Reputation of node j from the perspective of node i

- **Why beta distribution?**
  - **Simple** to store: Just characterized by 2 parameters.
  - **Intuitive**: α and β represents magnitude of cooperation and non-cooperation.
  - **Efficient**: Easy reputation updates, integration, trust formulation.

- **Maintain reputation for just neighboring nodes**

  Use **locality** – Provides **scalability**

2. Dual trust scheme

Most of current trust management models use dual evaluation or zone [0, 1] for evaluation (Yu, Singl, et al., 2004). Dual evaluation is not subjective, but it enables node to get a high trust value by a few successful transactions, which is vulnerable to outside attacks. So our model herein uses zone [0, 1] for evaluation, which enhances the pluralism of trust value and also ensures the continuity of it. We set nodes initial trust value to be 0.5, and after several transactions, the trust value of honest nodes is close to 1 while that of malicious ones will drop to less than 0.5. There are some nodes called strategy nodes. They initially behave well and get high trust value after joining in networks. Afterwards, they start to behave maliciously, reducing QoS or providing dishonest feedback. The most common method to fight against these attacks is to implement punishment mechanism to decrease their trust value. However, some strategy nodes only offer dishonest feedback but without reducing their own QoS. If single trust is employed, the trust value of these nodes will decrease sharply and cannot show their service abilities.

In view of the situation above, we set two trust values, for each node in our model. One is service trust value (STV),

providing the global trust value of the service; the other is request trust value (RTV), providing the global trust value of the evaluation. Both sides evaluate each other and update STV and RTV after each transaction. This dual trust values strategy is more flexible to fight against the attacks. We here set an example to illustrate the execution process of dual trust values in detail, shown in Fig. 2:

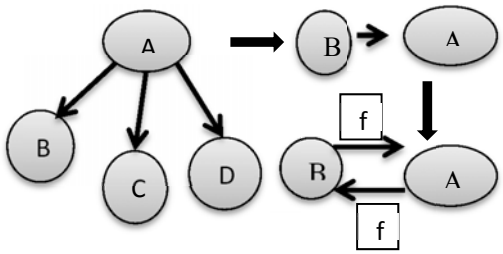


Fig2. Execution process of Dual Trust Values.

1. Supposing that node A has sent out a resource request and node B, C, and D have received it. They start to analyze the request and make response according to their own strategies (The analysis here includes evaluating the RTV of node A, checking whether they have such resource, etc.).
2. Node A will select the node with the highest trust value (for instance, here is node B) in terms of the local trust value (LTV: this trust value is STV stored locally, and it exists if transactions happened between them, otherwise it is set default) and the STV of responding node.

3.After selecting node B, node A will give node B an evaluation 'r' based on the transaction and its own strategies (for example, whether it is a malicious node or whether the response contains malicious information) Meanwhile, node B will give a feedback 'f' to node A as well.

4. Based on the feedback node A gives to node B, node A will calculate and update the STV of node B and save it as LTV as well.

5.Meanwhile, according to the feedback node B gives to node A, node B will calculate and update the RTV of node A.

5. Expected outcomes

(i) Mobility based intrusion detection which overcomes the issues of ambiguous collision.
(ii) False misbehavior detection by analyzing the identity and behavior of nodes.
(iii) Partial drops are detected through a central monitoring node.
(iv) Secure transmission and cooperative attack detection.
(v) Packet dropping and flooding preemptions removal.
(vi) Forging attack is timely measured with data analysis module through collector and transmission data storage.

Advantages:

1) Our proposed work differ from the existing work and by using the Eigen trust and Degree centrality concepts we can have individual trust claims and take routing decisions easily with minimum time.
2) Our reputation based security protocol is concerned with the active black hole attack with cryptographic techniques like Digital signature and hashing techniques.
3) Avoids the wastage of network resources and increase the network life time.
4) The applications like eCommerce: eBay, Email:anti-spam techniques, Personal Reputation: PersonRatings.com, we can provide more security.

6. Conclusion

Since mobile ad hoc network is an decentralized network with no fixed infrastructure security issues are the main area of interest. The proposed work gives an elaborative frame work for handling the security issues in the reputation based way. An adaptive decision boundary algorithm is used to classify the selfish nodes and malicious nodes from the regular nodes. The reputation based approach to the nodes uses the Eigen trust and Degree centrality concepts. The dual trust value for the nodes helps the trust evaluation process with different scenario into consideration. A detailed simulation evaluation will be conducted in terms of Routing Packet Overhead, Security Analysis, Mean Time to detect dropper node, Overall Network Throughput, and Average Latency.

8. References

[1] Akhtar and G. Sahoo, "Classification of Selfish and Regular Nodes Based on Reputation Values in MANET Using Adaptive Decision Boundary," *Communications and Network*, Vol. 5 No. 3, 2013, pp. 185-191. doi:10.4236/cn.2013.53021.

[2] S. S. Park, J. H. Lee, and T. M. Chung, "Cluster-based trust model against attacks in ad-hoc networks," in *Third International Conference on Convergence and Hybrid In63formation Technology*, pp. 526–532, 2008.

[3] Gagandeep, Aashima, Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" in International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[4] D. Ganesh and M. Sirisha "Reputation and Trust Evaluation in MANETs Using Eigen Trust Algorithm" in VSRD- IJCSIT, Vol. 2 (3), 2012, 175-189.

[5] Ceronmani Sharmila , Komala Valli "Enhanced Security through Agent Based Non-Repudiation Protocol for Mobile Agents" in International Journal of Power Control Signal and Computation (IJPCSC) Vol3. No1. Jan-Mar 2012.

[6] Kulbir Nain, Poonam Kumari, Roshan Lal Hiranwal "Improved DSR Protocol using Repudiation Based" in Journal of Computer Networking, Wireless and Mobile Communications (JCNWMC) Vol.2, Issue 1 Sep 2012 7-15.

[7] Mohammed Mujeeb, Sudhakar K N, Jitendranath Mungara "Reputation-Based Security Protocol for MANETs" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-2, July 2012

[8] S.Sasikala and M.Vallinayagam, ―Secured Intrusion Detection System in Mobile Ad Hoc Network using RAODV ―, in Proceedings published in International Journal of Computer Applications (IJCA), ISSN: 0975 – 8887, ICRTCT-2013

[9] S. Ramaswamy et al, "Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks," ICWN'05, 2005, pp. 595-604.

[10] S.Sasikala and M.Vallinayagam, ―Secured Intrusion Detection System in Mobile Ad Hoc Network using RAODV ―, in Proceedings published in International Journal of Computer Applications (IJCA), ISSN: 0975 – 8887, ICRTCT-2013.

[11] Sagar Pandiya, Rakesh Pandit and Sachin Patel, ―Survey of Innovated Techniques to Detect Selfish Nodes in MANET‖, in International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), ISSN 2250-1568, Vol. 3, Issue 1, Mar 2013, 221-230.