International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
Volume 2 Issue 1 –OCTOBER 2013.

An Evidence Collection Trust based Risk free routing attacks in MANET

A. Pratapa Reddya[#1], Dr. N. Satyanarayana[*2]

[#]*Associate Professor, Dept. of CSE, GanapthyEngineering College, Warangal, AP*
[1] prathapreddy54@gmail.com
[*]*Professor, Dept. of CSE, Nagole Institue of Science & Technology, AP*

***Abstract*- Mobile ad hoc networks (MANETs) consists of group or set of mobile nodes which are self-configuring and joined by wireless communication networks links routinely as per the distinct steering protocol. MANET is the infrastructure less networks and has no centralized server to control the mobile nodes in the networks. The important feature of MANETs is the absence of a fixed infrastructure but mobile nodes involves networks and all the nodes are mobility in nature. Though the MANET works efficiently in different ways, the routing protocol attacks or intermediate nodes attacks in the Mobile Ad Hoc networks is the important issues. To address these issues in the MANET the author proposed a risk-aware response mechanism to analytically handle with routing attacks in Mobile Ad Hoc Networks. And also one previous approach has intrusion detection systems (IDS). This approach proposed for to address the routing protocol attacks in the MANET but mechanisms that are insufficient to give the current obstacles. In order to overcome the routing attacks in the mobile ad hoc networks, we proposed new effective technique with the idea of the previous approach using Risk Aware Mechanism. In this paper we proposed a new technique to perceive the routing attacks with reply or alert system by using the delivery packets ratio between the nodes in the MANET. Our proposed technique also addresses the replica attacks in the mobile ad hoc networks. Our proposed system works effectively and efficiently when compared to the previous approaches, it shown through our simulation and result analysis.**

***Index Terms*- Mobile ad hoc networks, replica nodes, intrusion response, adaptive decision making, delivery packets, time domain ratio and distance nodes.**

I. INTRODUCTION

Mobile computing [1] is the discipline for creating an information management platform, which is free from spatial and temporal constraints. The freedom from these constraints allows its users to access and process desired information from anywhere in the space. The state of the user, static or mobile, does not affect the information management capability of the mobile platform. A user can continue to access and manipulate desired data while travelling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, where as in reality they may be located far away.

Though the MANET works efficiently in different ways, the routing protocol attacks or intermediate nodes attacks in the Mobile Ad Hoc networks is the important issues. To address these issues in the MANET the author proposed a risk-aware response mechanism to analytically handle with routing attacks in Mobile Ad Hoc Networks. There are many several previous work try to address the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviours like false statement of node ID and cloning of Nodes and so on. Such an uncomplicated reply against wicked nodes frequently rejects the possible negative side effects involved with the response actions in the mobile networks. In the mobile ad hoc networks scenario, inappropriate oppose events may origin the unforeseen network separation, bringing additional reparation to the system infrastructure totally. To overcome the above-mentioned serious obstacles in the MANET, more stretchy and adaptive intimation scheme should be investigated. The concept of risk aware in the mobile networks can be adopted to support more effective responses to routing protocol attacks. Still, risk assessment in the MANET is still a nontrivial, challenging issue due to its involvements of prejudiced information, objective verification, and logical reasoning.

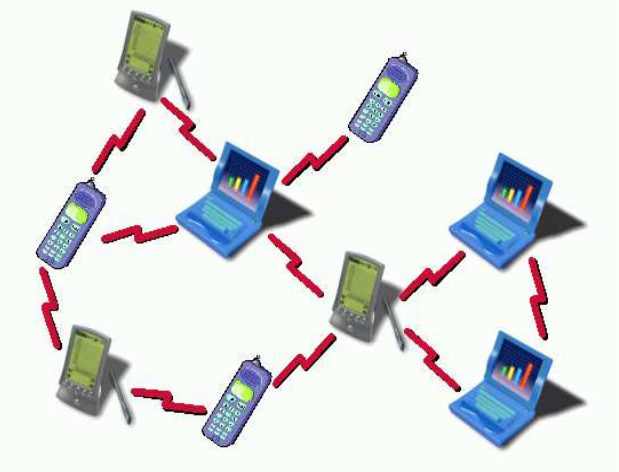

Figure.1 Architecture of Mobile Ad Hoc Networks (MANET)

Above network will not crumple since one of the mobile nodes moves out of transmitter range. Nodes be obliged to be able to penetrate/disappear from the network due to nodes have limited transmission range. To achieve the other nodes, several hops will be desired. Therefore, every node try to participate in a Mobile ad-hoc network must be willing to forward packets for other nodes. Any compromised nodes under the attacker's control could cause momentous hurt to the functionality and protection of its network since the collision would propagate in performing routing protocol tasks.

In order to overcome the routing attacks in the mobile ad hoc networks, we proposed new effective technique with the idea of the previous approach using Risk Aware Mechanism. In this paper we proposed a new technique to observe the routing attacks with reply or alert system by using the delivery packets ratio between the nodes in the MANET. Our proposed technique also addresses the replica attacks in the mobile ad hoc networks. Replica Attacks is a challenge by the adversary to add one or more nodes to the network circle that use the same ID as another node in the network. In order to identify the Replica attacks in the MANET, we using Location Information Exchange protocol and Time Domain Detection & Space Domain Detection Scheme. Both schemes are used to identify the replica attacks in the mobile ad hoc networks. Our proposed system works effectively and efficiently when compared to the previous approaches, it shown through our simulation and result analysis.

The rest of the paper will be organised as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The algorithms and simulation are shown in the section 4 and 5. The conclusion of our paper is in section 6.

II. Related Works

In this section, we will see the some of the related works to the intrusion detection system using different approaches:

Wenjia Li and Anupam Joshi [2], in this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.

Po-wah yau, shenglan hu and chris j. mitchell [2], the main purpose of an ad hoc network routing protocol is to enable the transport of data packets from one point to another. This paper examines the potential attacks on this transport service which arise from the realisation of threats from internal malicious nodes. The prerequisite of a routing service is a distributed mechanism for the discovery and maintenance of routes; network integrity and availability are required to ensure the correct operation of an ad hoc network. This paper also provides a qualitative analysis of how proactive and reactive protocols cope with malicious internal attacks, and whether one type of protocol offers inherently better resistance to the various attacks than the other.

A.Anna lakshmi and Dr.K.R.Valluvan [3], Mobile Ad hoc Network is the kind of wireless networks that utilize multi-hop radio relaying and it is an infrastructure less Network due to its capability of operating without the support of any fixed infrastructure. Security plays a vital role in mobile ad hoc network (MANET) due to its applications like battlefield or disasterrecovery networks. Current wireless research points out that the wireless MANET has more security problems than traditional wired and wireless networks. MANET is severely affected by Distributed Denial of Servic e (DDoS) attacks which becomes a problem for users of computer systems connected to the Internet. MANETs are more vulnerable compared to wired networks due the lack of a trusted centralized authority and limited resources. This paper discusses various attacks on MANET and defense mechanisms for DDOS attacks in MANET as reported in the literature.

Yih-Chun Hu, Adrian Perrig and David B. Johnson [4], As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper we introduce the wormhole attack, a severe attack in ad hocnetworks that is particularly challenging to defend against.The wormhole attack is possible even if the attacker has notcompromised any hosts, and even if all communication providesauthenticity and confidentiality . In the wormhole attack, anattacker records packets (or bits) at one location in the network,tunnels them (possibly selectively) to another location, andretransmits them there into the network. The wormhole attackcan form a serious threat in wireless networks, especially againstmany ad hoc network routing protocols and location-basedwireless security systems. For example, most existing ad hocnetwork routing protocols, without some mechanism to defendagainst the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication.We present a new, general mechanism, called packet leashes, fordetecting and thus defending against wormhole attacks, and wepresent a specific protocol, called TIK, that implements leashes.

Bryan Parno, Adrian Perrig and Virgil Gligor [5], The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locationswithin the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with singlepoints of failure, or on neighborhood voting protocolsthat fail to detect distributed replications. To addressthese fundamental limitations, we propose two new algorithms based on emergent properties, i.e., properties that arise only through the collective action ofmultiple nodes. Randomized Multicast distributes nodelocation information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes,while Line-Selected Multicast uses the topology of thenetwork to detect replication. Both algorithms provide globally-aware, distributed node-replica detection,and Line-Selected Multicast displays particularly strongperformance characteristics. We show that emergent algorithms represent a promising new approach to sensornetwork security; moreover, our results naturally extendto other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu [6],mobile Ad hoc Networks (MANET) have beenhighly vulnerable to attacks dueto thedynamic nature of itsnetwork infrastructure. Among these attacks, routing attack shave received considerable attention since it could cause the most devastating damage to MANET. Even though there exist several intrusion response techniques to mitigate such critical attacks,existing solutionstypically attempt to isolate malicious nodesbased on binary or na¨ıve fuzzy response decisions. However, binary responses may result in the unexpected network partition,causing additionaldamages to the network infrastructure, andna¨ıve fuzzy responses could lead to uncertainty in counteringrouting attacks in MANET. In this paper, we propose a riskaware response mechanism to systematically cope with theidentified routing attacks. Our risk-aware approach is based onan extended DempsterShafer mathematical theory of evidenceintroducing a notion of importance factor. In addition, ourexperiments demonstrate the effectiveness of our approach withthe consideration of the packet delivery ratio and routing cost.

III. PROPOSED WORK

In order to overcome the routing attacks in the mobile ad hoc networks, we proposed new effective technique with the idea of the previous approach using Risk Aware Mechanism. In this paper we proposed a new technique to observe the routing attacks with reply or alert system by using the delivery packets ratio between the nodes in the MANET. Our proposed technique also addresses the replica attacks in the mobile ad hoc networks. Replica Attacks is a challenge by the adversary to add one or more nodes to the network circle that use the same ID as another node in the network. In order to identify the Replica attacks in the MANET, we using Location Information Exchange protocol and Time Domain Detection & Space Domain Detection Scheme. Both schemes are used to identify the replica attacks in the mobile ad hoc networks. Our proposed system works effectively and efficiently when compared to the previous approaches, it shown through our simulation and result analysis.

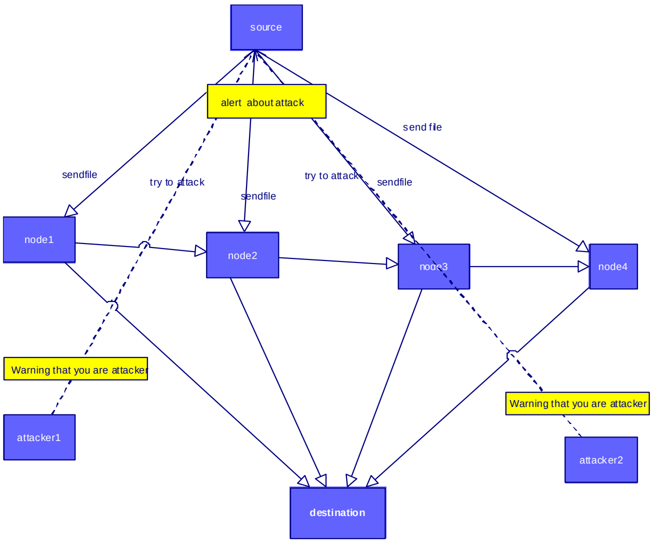

Figure 2: Flow of the system

IV. Simulation Works

We have simulated our system in Java. We implemented and tested with a system configuration on Intel Dual Core processor, Windows XP and using Netbeans 7.0. We have used the following modules in our implementation part. The details of each module for this system are as follows:

1) Evidence collection

In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

2) Risk assessment

Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

3) Decision making

The adaptive decision module provides a flexible response decision making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.

4) Intrusion response

With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

5) Routing table recovery

Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In proactive routing protocols like OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

V. Conclusion

Our proposed techniques in this paper, address to address the routing protocol attacks in the MANET. In this paper we proposed a new technique to observe the routing attacks with reply or alert system by using the delivery packets ratio between the nodes in the MANET. Our proposed technique also addresses the replica attacks in the mobile ad hoc networks. Replica Attacks is a challenge by the adversary to add one or more nodes to the network circle that use the same ID as another node in the network. In order to identify the Replica attacks in the MANET, we using Location Information Exchange protocol and Time Domain Detection & Space Domain Detection Scheme. Both schemes are used to identify the replica attacks in the mobile ad hoc networks our proposed technique is also applied for the securing purposes in the mobile ad hoc networks. Our experimental result showed that our proposed novel technique works efficiently when compared to previous methods.

VI. References

[1] Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald ‘Privacy-Aware Location Sensor Networks”

[2] Osman Yağan, Member, IEEE, and Armand M. Makowski, Fellow, IEEE “Modeling the Pairwise Key Predistribution Scheme in the Presence of Unreliable Links”- IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 59, NO. 3, MARCH 2013

[3] Min Shao, Yi Yang, Sencun Zhu, Guohong Cao “Towards Statistically Strong Source Anonymity for Sensor Networks”- This paper was originally published in the Proceedings of HotOS IX: The 9th Workshop on Hot

[4] Mauro Conti, Lei Zhang, Sankardas Roy, Roberto Di Pietro, Sushil Jajodia,Luigi Vincenzo Mancini “Privacy-preserving robust data aggregation in wireless sensor networks” Article first published online: 14 JAN 2009

[5] Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham “Privacy preservation in wireless sensor networks: A state-of-the-art survey”

[6] Clark, A. Cuellar, J Poovendran, R “Statistical Framework for Source Anonymity in Sensor Networks”

[7] Di Ma ; Tsudik, G “Security and privacy in emerging wireless networks”

[8] Jiri Kiur “Privacy preserving protocols for wireless sensor networks”-

[9] H. Wang, B. Sheng, and Q. Li, “Privacy-Aware Routing in Sensor Networks,”Elsevier J. Computer Networks,vol. 53, no. 9, pp. 1512-1529, 2009.

[10] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, “Cross-Layer Enhanced Source Location Privacy in Sensor Networks,” Proc. IEEE Comm. Soc. Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON ’09), pp. 324-332, 2009.

[11] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, “Query Privacy in Wireless Sensor Networks,” ACM Trans. Sensor Networks,vol. 6, no. 2, pp. 1-34, 2010.

[12] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks,”IEEE J. Selected Areas in Comm.,vol. 28, no. 5, pp. 677-691, June 2010.

[13] S. Goldwasser and S. Micali, “Probabilistic Encryption,” J. Computer and System Sciences,vol. 28, no. 2, pp. 270-299, 1984.

[14] T. Anderson and D. Darling, “Asymptotic Theory of Certain ‘Goodness of Fit’ Criteria Based on Stochastic Processes,” The Annals of Math. Statistics,vol. 23, no. 2, pp. 193-212, 1952.

[15] F. Massey Jr., “The Kolmogorov-Smirnov Test for Goodness of Fit,”J. Am. Statistical Assoc.,vol. 46, no. 253, pp. 68-78, 1951.

[16] C. Jarque and A. Bera, “A Test for Normality of Observations and Regression Residuals,”Int’l Statistical Rev./Revue Internationale de Statistique,vol. 55, no. 2, pp. 163-172, 1987.

[17] S. Golomb and G. Gong, Signal Design for Good Correlation. Cambridge Univ., 2005.

[18] L. Scharf,Statistical Signal Processing: Detection, Estimation, and Time Series Analysis.Addison-Wesley, 1991.

[19] H. Karl and A. Willig,Protocols and Architectures for Wireless Sensor Networks.Wiley, 2005.

[20] Q. Gu, X. Chen, Z. Jiang, and J. Wu, “Sink-Anonymity Mobility Control in Wireless Sensor Networks,”Proc. IEEE Fifth Int’l Conf. Wireless and Mobile Computing, Networking and Comm. (WiMob ’09), pp. 36-41, 2009

A Pratapa Reddy obtained his Bachelor of Technology degree in Mechanical Engineering from Kakatiya University, Warangal, A.P. Then he obtained his Master of Technology degree in Computer Science & Engineering from JNTUH, Hyderabad, A.P. and pursuing PhD in Computer Science & Engineering from JNTUH, Hyderabad, A.P. Currently, he is a Assoc. Prof. at the Department of Computer Science and Engineering, Ganapathy Engineering College, Warangal, A.P. His specializations include networking, MANET, Network Security. His current research interests are wireless communications and networking, MANET, Network Security.

Dr.N.Satyanarayana, M.Sc, M.Phil, AMIE(ET), M.Tech (CS), Ph.D (CSE), MISTE,MCSI, received his Ph.D degree in Computer Science & Engineering from Acharya Nagarjuna University, currently working as a Professor in department of CSE at Nagole Institute Of Science & technology. His research interests include Advanced Computer Architecture, Networking, and Wireless Communications