International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 1 –JULY 2014.

By Using Effective Mechanism for Detection and Prevention of Routing Attacks in Mobile Networks

[1*] K. Meghana, and [2#] K. Manohar

[1]*M.E(CSE), Audishankara College of Engineering and Technology, Gudur, Andhra Pradesh*

[2]*Associate Professor(CSE), Audishankara College of Engineering and Technology, Gudur, Andhra Pradesh*

***Abstract*— In Recent days in the group mobile user's communication, group key management was found to be challenging in the decentralized environments because of its dynamic nature. Even though many existing solutions have been proposed to switch key changes for character mobile user's or crowds, in this paper gives the characteristics of rekeying achieved by those methods. In the previous existing scheme the principal sanctuary mechanism of group statement is achieved by conservative encryption algorithms, in which key delivery and rekeying maintained of the group key was done by Group organizer. Though it produces the efficient rekeying framework for the group management, it fails to produces the effective results against routing attacks in Mobile Networks. Mobile ad hoc networks (Wireless Mobile Networks) 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. Wireless Mobile Networks is the infrastructure less networks and has no centralized server to control the mobile nodes in the networks. The important feature of Wireless Mobile Networks is the absence of a fixed infrastructure but mobile nodes involves networks and all the nodes are mobility in nature. Though, the Wireless Mobile Networks works efficiently in different ways, the routing protocol attacks or intermediate nodes attacks in the Mobile networks is the important issues. To address these issues we proposed a risk-aware response mechanism to analytically handle with routing attacks in Mobile Networks. In order to overcome the routing attacks in the mobile ad hoc networks, we proposed new effective technique with the idea of the previous approaches 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 entire Networks. Our proposed system works effectively and efficiently when compared to the previous approaches, it shown through our simulation and result analysis.**

***Keywords*— 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 Wireless Mobile Networks 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 Wireless Mobile Networks 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 Wireless Mobile Networks 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 Wireless Mobile Networks, 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 Wireless Mobile Networks is still a nontrivial, challenging issue due to its involvements of prejudiced information, objective verification, and logical reasoning.

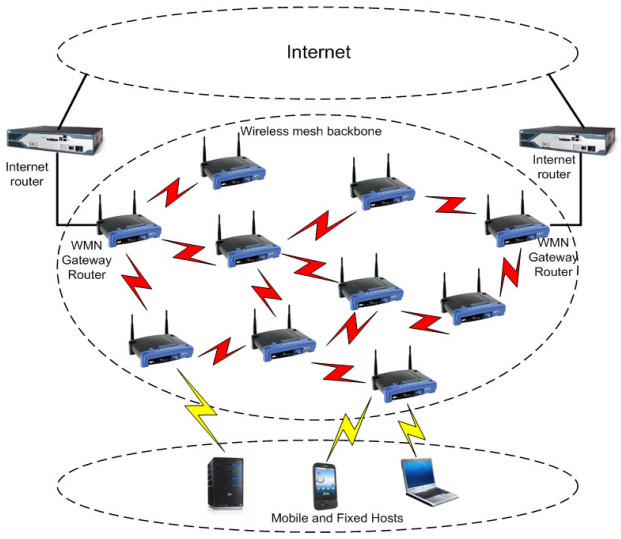

Figure.1 Architecture of Mobile Ad Hoc Networks (Wireless Mobile Networks)

Above network will not rumple ever since one of the mobile nodes be in motion out of transmitter assortment. 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 arrangement must be prepared to advance packets for extra 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 Wireless Mobile 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 conclusion of our paper is in section 5.

II. RELATED WORKS

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

Matthias Grossglauser and David N. C. Tse [1], the capability of ad hoc wireless networks is forced by the common intrusion of concomitant communication between the two nodes. We study a model of a wireless ad hoc network where nodes correspond in arbitrary to the resource–target pairs. These wireless nodes are tacit to be mobile for the communication networks. We examine the each and every session throughput for the wireless network applications with variable stoppage constraints, such a wireless network topology changes or clear in excess of the instant scale of packet or data's delivery. Under this statement, the per-user throughput can augment radically when nodes are movable moderately than fixed. This development can be achieved through by exploiting an appearance of multiuser multiplicity via sachet or information relaying between the two different nodes.

Shuo Guo, Ziguo Zhong and Tian He [2], wireless Sensor Networks are typically huge compilation of sensor nodes for cumulative of data or information as of watching the surroundings and broadcast to base position through multi-hop wireless message of nodes. The present of faults nodes in the WSNs are extremely lofty owing to wireless contact and unsystematic operation strategy. Force protection in wireless sensor network is an extra issue is to get better applicability of WSNs (wireless sensor networks). In order to overcome the above issues, we recommend division based Misbehaviour nodes identify and revival technique, which is as well as energy knowledgeable. In the above proposed technique, sensor nodes are agreed into several clusters. Cluster start and wireless sensor nodes are together for perceive the fault in the sensor nodes. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

B. Umakanth and J. Damodhar[3], Wireless Sensor Networks came to importance approximately the begin of this millennium provoked by the ubiquitous situation of small-sized sensors with limited range control deployed in the huge information over an vicinity to examine different occurrence. The solitary motivation of a large segment of investigate efforts has been to exploit the lifetime of the wireless network, where network lifetime is typically measured from the immediate of consumption to the peak when one of the nodes has exhausted its partial power source and become in-operational – normally referred since first node collapse. In excess of the time, research has increasingly adopted ideas from wireless communications. In this paper we consider how routing protocols, affect from

attack even those designed to be protected, be short of security from these attacks, which we call Vampire attacks in the wireless networks, which permanently immobilize networks by quickly misbehaviour nodes' of draining the sequence energy. These type of "parasite" attacks are not specific to any specific protocol which are overwhelming, not easy to identify, and are easy to bring out using as few as one wicked insider sending only procedure acquiescent messages. We proposed a EWMA method to bound the damage caused by these vampire types of attacks during the packet forwarding phase.

Zinaida benenson , Peter M. cholewinski and, Felix C. freiling [4], We examine how wireless ad hoc networks can be attacked in follow. Beginning of this, we extend our previous idea of generic rival model that allows classifying the adversaries according to the two extent of power: presence and intervention. Thus, we provide a framework for realistic safety measures analysis in wireless sensor or ad hoc networks

Chris Karlof and David Wagner [5], we examine the routing protocol security in wireless networks. Many wireless sensor network routing protocols comprise be proposed in previous, but nothing of them have been considered with security as a goal in the wireless networks. We propose the effective protection goals for routing protocols in the sensor networks, show how attacks beside ad-hoc and end to end networks can be adapted into dominant attacks against sensor networks, initiate two classes of novel attacks touching sensor networks —sinkholes and HELLO floods, and we analyse that the security of all the major sensor network routing protocols. We illustrate crippling attacks against all of them and propose countermeasures and aim for considerations. This is the first such examine of secure routing in wireless sensor networks.

Farhad Nematy , and Naeim Rahmani [6], in modern years there has been a growing consideration in wireless ad hoc sensor networks (WSN) applications. Such wireless sensor networks are able to be second-hand to manage temperature in the desert or volcanic regions, humidity, contamination, pollution etc. Energy utilization and dependability are two serious issues in WSNs. Faults or Misbehaviour occurring to sensor nodes is frequent owing to be short of power or ecological intrusion. In this paper recovery of faults nodes or misbehaviour in cluster beginning deliberate and genetic system is used to recuperate huddle members to other cluster heads. Our Simulation results show effectiveness that proposed genetic algorithm can recover the fault nodes efficiently.

Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu [7],mobile Ad hoc Networks (Wireless Mobile Networks) have beenhighly vulnerable to attacks dueto thedyn amic nature of itsnetwork infrastructure. Among these attacks, routing attack shave received considerable attention since it could cause the most devastating damage to Wireless Mobile Networks. Even though there exist several intrusion response techniques to mitigate such critical attacks, existing solutionstypically attempt to isolate malicious nodesb ased on binary or na¨ıve fuzzy response decisions. However, binary responses may result in the unexpected network partition,causing additionaldamages to the network infrastruct ure, andna¨ıve fuzzy responses could lead to uncertainty in co unteringrouting attacks in Wireless Mobile Networks. In this paper, we propose a riskaware response mec hanism to systematically cope with theidentified routing attacks. Our risk-aware approach is based onan extended DempsterShafer mathematical theory of eviden ceintroducing a notion of importance factor. In addition, ourex periments 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 Wireless Mobile Networks.

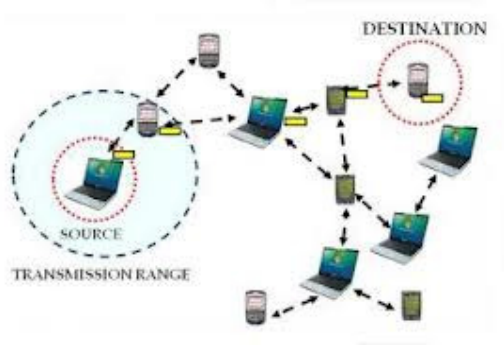

Figure 2- Risk Aware Migitation in Mobile Networks

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 using the same ID of the mobile node as compared to another node in the network. In order to identify

the Replica attacks in the Wireless Mobile Networks, 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.

IV. ALGORITHM

Algorithm for Routing Attacks Detection:

Training:

Step 1: Select the number of nodes, n, for the complete system.
Step 2: Generate Network key generation.
Step 3: IP Verification
Step 4: Check Protocol audit specific to each layer
Step 5: Plug in the trained copy successively such that only the connections labelled as ordinary are accepted to the next layer based on PDR.

Testing:

Step 6: For each (next) test occurrence perform Steps 8 to 10.
Step 7: Test the incident and label it moreover as assault or standard.
Step 8: If the occurrence is labelled as assault, obstruct it and categorize it as an attack symbolize by the layer name at which it is identified and go to Step 7. Else pass the progression to the next layer of the communication.
Step 9: If the current layer is not the last layer in the system, test the occurrence and go to Step 9. Else go to Step 10.
Step 10: Test the instance and label it either as normal or as an attack. If the instance is labelled as an attack, block it and identify it as an attack corresponding to the layer name

V. CONCLUSION

Our proposed techniques in this paper, address to address the routing protocol attacks in the Wireless Mobile Networks. 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 Wireless Mobile Networks. 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 Wireless Mobile Networks, 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 alert Location Sensor Networks"
[2] Osman Yağan, Member, IEEE, and Armand M. Makowski, Fellow, IEEE "Modeling the Pairwise Key Predistribution method 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 resource 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 protection in wireless sensor networks: A state-of-the-art survey"
[6] Clark, A. Cuellar, J Poovendran, R "geometric structure for Source Anonymity in Sensor Networks"
[7] Di Ma ; Tsudik, G "protection 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