ISSN No: 2348-4845

International Journal & Magazine of Engineering, Technology, Management and Research

A Peer Reviewed Open Access International Journal

Malicious-Behaviour-Detection in MANETS Using Enhanced Adaptive Acknowledgment

Golla Subramanyam
Persuing M.Tech,
Dr.K.V.Subba Reddy Institute of Technology.

C.Md Gulzar
Associate Professor,
Dr.K.V.Subba Reddy Institute of Technology.

Abstract:

Many research works have been done to prevent the vulnerabilities of MANETs. But there is still unexplored nooks and corners are left for locking. To face the challenges in preventing the intruders attacks an efficient Enhanced Adaptive ACKnowledgment mechanism or technique is given in this research work. This Enhanced Adaptive ACKnowledgment IDS is developed and proposed to detect higher malicious behaviour in certain circumstances and situations in the Mobile Ad hoc NETworks.This research work is simulated in .Net technologies to replicate the Mobile Ad hoc networks vulnerabilities and demonstrate the admeasures against different malicious attacks with its Enhanced Adaptive ACKnowledgment. The simulation results are properly demonstrated to revel the effective admeasures provided by the Intrusion Detection System enriched with Adaptive ACKnowledgment algorithms.

Keywords:

MANETs, malicious attacks in Networks, safety and security.

Introduction:
Background:

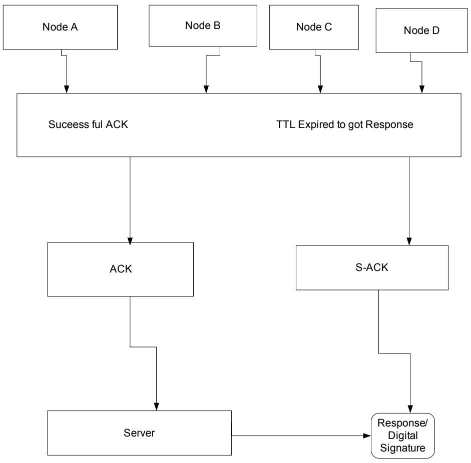
Wireless networks are primary option from first day of their invention due to their natural mobility and scalability.Due to the technology improvement and to reduce cost, we prefer wireless network over wired networked since few years. Our title says, Mobile Ad hoc NETwork (MANET) is a group of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. The organizational remote access and control via wireless networks are becoming more and more popular these days (Kim et al., 2008). because of MANET's distributed scenario and changing topology, (Patwardhanet al., 2005)a traditional decentralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially developed for MANETs. Many research efforts have been devoted to such research topic(Al Agha et al., 2009)–(Akbaniet al., 2012),

AIM OF THE PROJECT:

The main aim of the project is to identify the effected nodes (i,e., malicious nodes) in Mobile Ad Hoc Networks(MANETS) using a Enhanced Adaptive ACKnowledgment [EAACK]technique which is developed for Higher Intrusion-Detection. The effected nodes are infected by the malicious attacker influence to distribute the vulnerabilities in the network. This abnormal behavior should be stopped and protect the other nodes of MANET from attacks.

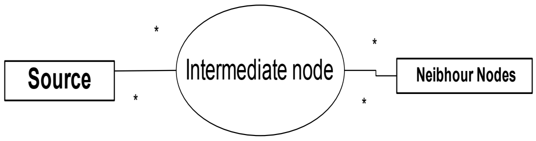
Design of the project:

The present project is on Vision on Vulnerabilities in Delay Tolerant Networks. The design of the project is determined from the analysis of the requirements of the project. The design consists of mainly two parts. One is User Interface Screens Design and the other is Database Design. The present project is a simulation project, hence the database design is avoided. Most of the networking projects don't configured with database. The proposed project is built with user interface Screens and business logic to replicate the functionality of the project.

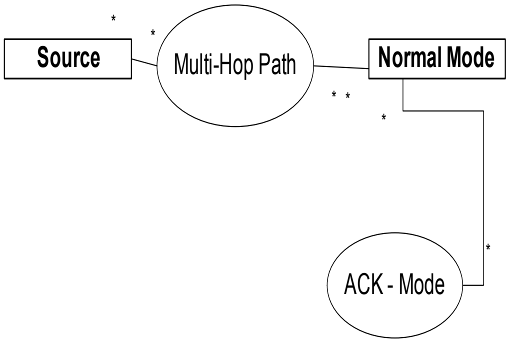


In the above picture the server will receive the data from node one node two, node three and node four. Once the nodes are sending the data this will be demonstrated by TTL expressions. If the data is transmitting from node it will be reflected in TTL values. If the TTL value is greater than equal to 32 it will be transmitted from a node. Then it will be passing through intermediate node which implements the Enhanced Adaptive ACKnowledgment system. Then the data packets are transmitted to the server system. The server system will be considered as Destination Nodes and the clients are considered as source nodes. When the server is responding for the requests sent from clients it should be verified with digital Signature of the client systems to apply security.

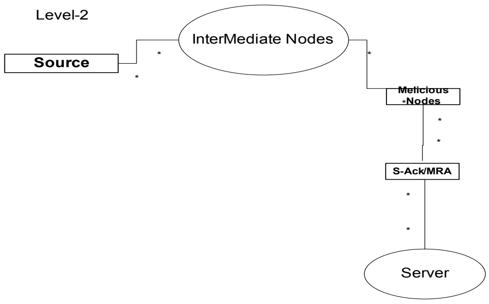
Level 0



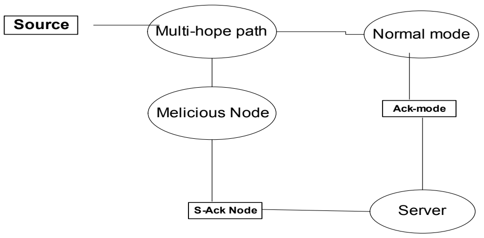
Level-1



Delay Tolerant Networks are configured with dynamic nodes. The transmission between one node to other node will get delay. To increase the performance of the transmission speed, the intermediate node is configured. The intermediate node increase the buffer size to store the data and send the data to the destination node. The transmission of electronic data packets is increased with the presence of intermediate node and makes the transaction continuous. Level 1 indicates the configuration of enhanced adaptive ACKnowledgment mechanism to audit the data packets for its source destination address and acknowledge the same and sent the data to the servers. This will also speed up the transmission and makes the connectivity continuous. In the level 1 it is a safe and secure transaction to avoid the vulnerabilities in the network.



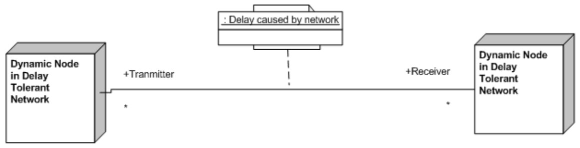
Level-3



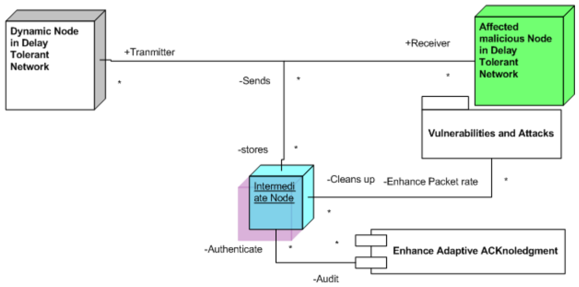
The above picture demonstrate the functionality of the AcKNOWLEDGEMENT methodology is working to remove the infections of the network. Once the data packetsare released from source node, they will be transmitted through intermediate node. The intermediate node will identify the malicious nodes caused by the attacks of intruders. The data packets will be edited by the ACK mechanism and send the data packets if they are coming from authorised and authenticated node. Level 3 demonstrate the ACK mechanism in case of data packets are starting from multi hop environment. In this s Level 3 demonstrate the ACK mechanism in case of data packets are starting from multi hop environment. In this scenario the ACK mechanism will audit and authenticate the data packets. If the data packets are coming from authenticated and authorised node then the data packets are sent to server system. While the reply and response is sending from server it also follows the same method to transmit the data packets to the destination node [client]. cenario the ACK mechanism will audit and authenticate the data packets. If the data packets are coming from authenticated and authorised node then the data packets are sent to server system.

While the reply and response is sending from server it also follows the same method to transmit the data packets to the destination node [client].

Existing System


: Delay caused by network
Dynamic Node in Delay Tolerant Network
+Tranmitter
+Receiver
Dynamic Node in Delay Tolerant Network

Proposed System


Dynamic Node in Delay Tolerant Network
+Tranmitter
+Receiver
Affected malicious Node in Delay Tolerant Network
-Sends
Vulnerabilities and Attacks
-stores
Intermedi ate Node
-Cleans up
-Enhance Packet rate
-Authenticate
Enhance Adaptive ACKnoledgment
-Audit

Results:

Present project is vision of vulnerabilities in delay tolerant networks. The present project is a simulation project to demonstrate the functionality of the delay tolerant networks. The project is developed to demonstrate the DTN environment with the configuration of nodes, routers, attackers, vulnerabilities and intrusion detection systems. The project should simulate the functionality of dynamic nodes. The project should demonstrate the functionality of the routers. The project should reveal the functionality of the attackers. The simulation environment should demonstrate the attackers functionality and the functionality of the admeasures configured in intrusion detection system. The intrusion detection system is enriched with enhanced adaptive acknowledgement mechanism to audit the intruders source address and authenticate the data packets. The results of the project can be enlisted below.
The data transmission between the nodes should be demonstrated - Yes Demonstrated
The delay tolerance between two nodes should be counted - Yes Estimated
The vulnerabilities should be activated Yes Activated
The delay count should be recorded from infected node - Yes counted
The data packet transmission rate should be counted
Before infection .01 sec
After infection .9 sec
After ACK enforcement .001 Sec

Evaluation of results:

The evaluation of results revel that, the delay tolerance networks are transmitting the electronic data packets with remarkable delay. The intrusion and malicious attacks can affect the system and cause great delay in transmission and also packet loss.The intrusion detection system with EAACK method has stopped the intrusions and improved the packet transmission speed.The intrusion detection system with EASCK method has reduced the packet loss.

Conclusion:

Delay Tolerant Networks are very important in the fields of rural education and space networks. The importance has increased as DTN is predominantly first option for space networks to transmit the data from earth stations to space stations. The nodes configured in DTN are dynamically placed with multi-functional activities. The nodes in DTN are bound to break the connectivity and the delay in transmission is frequent and common. At this juncture the project has developed a vision for DTN for space networks. The present project is developed and demonstrated a vision to overcome the vulnerabilities in Delay Tolerant Networks. The project has demonstrated the intrusion detection system with the aid of Enhanced Adaptive Acknowledgement system to improve the speed of the data transmission, reduce the packet loss and to improve the bandwidth transmission with the help of intermediate node incorporation.

Elhadi M. Shakshuki, et.al [2013] The simulation project has successfully demonstrated the functionality of the project. The results have been recorded and evaluated. The results revealed that the project has successfully demonstrated the final output of intrusion detection system developed with the combination of watchdog and parthrater to verify the signatures of the electronic data packet transmission from one to other node in the networks. The remarkable improvement in transmission speed, predominant bandwidth increase and required data packets loss has been gained in this project execution.

The evaluated results revealed that the intrusion detection system has given a better vision for Delay Tolerance Networks. The project has fulfilled the objectives and goals specified in the introduction chapter.Elhadi M. Shakshuki, et.al [2013].

Reference:

1. Kim, Y.(2008) Remote sensing and control of an irrigation system using a distributed wireless sensor network,IEEE Trans. Instrum.Meas., vol. 57, no. 7, pp. 1379–1387.

2.Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE [2013] EAACK—A Secure Intrusion-Detection System for MANETs published IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

3.Jayakumar, G and Gopinath, G.(2007)Ad hoc mobile wireless networks routing protocol—A review,J. Comput. Sci., vol. 3, no. 8, pp. 574–582.

4.Sun, B. (2004) Intrusion detection in mobile ad hoc networks, Ph.D. dissertation, Texas A&M Univ., College Station, TX.

5.SevilŞen, John A. Clark [2007]Intrusion Detection In Mobile Ad Hoc Networksdownloaded from www-users.cs.york.ac.uk/~jac/PublishedPapers/IDinMANETs.pdf

6.Yi Ping, Jiang Xinghao1, Wu Yue1 & Liu Ning [2008] Distributed intrusion detection for mobile ad hoc networks published in Journal of Systems Engineerng and Electronics Vol. 19, No. 4, 2008, pp.851–859 downloaded from www.Sciencedirect.com/science/journal/10044132.

7.BalasubramanianShyamSundar [2012]Assessing The Vulnerability Of Dtn Data Relaying Schemes To Node Selfishness

8.Aniket Kate, Gregory M. Zaverucha, and UrsHengartner [2007]Anonymity and Security in Delay Tolerant Networks by 10.1109/SECCOM.2007.4550373 pages 504 - 513

9.Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker [2000]Mitigating Routing Misbehavior in Mobile Ad Hoc Networks Copyright ACM 2000 1-58113-197-6/00.

10.Sotirios-AngelosLenas, Scott C. Burleigh, and VassilisTsaoussidis[2012] Reliable Data Streaming over Delay Tolerant Networks Y. Koucheryavy et al. (Eds.): WWIC 2012, LNCS 7277, pp. 358–365, 2012. © Springer-Verlag Berlin Heidelberg 2012

11.CaseMaker [2000] Rapid Application Development @ Copyright 1997-2000 CASEMaker Inc.- E-Book Published in www.casemaker.com

12.Ulf Ekstrom [2000] Design Patterns for Simulations in Erlang/OTP - 2000-11-01 ISSN 1100{1836 Information Technology Computing Science Department

13.Tabesh andFrechette, L.G (2010) A low-power standalone adaptive circuit for harvesting energy from a piezoelectric micropower generator,IEEETrans. Ind. Electron., vol. 57, no. 3, pp. 840–849.

14.Nasser, N and Chen, Y. (2007) Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network, in Proc. IEEE Int.Conf. Commun., Glasgow, Scotland.

15.Glenn A. Bowen [2005] Preparing a Qualitative Research-Based Dissertation: Lessons Learned The Qualitative Report Volume 10 Number 2 June 2005 208-222 http://www.nova.edu/ssss/QR/QR10-2/bowen.pdf

16.Rolf Johansson [2003] Case Study Methodology - A key note speech at the International Conference

17.Sparx Systems [2004] UML TUTORIALS THE USE CASE MODEL copy right reserved © Sparx Systems 2004 published in www.sparxsystems.com.au

18.Steve Easterbrook, Janice Singer, Margaret-Anne Storey, Daniela Damian [2007] Selecting Empirical Methods for Software Engineering Published for Toronto edu 2007 September.

19.Ellen Taylor-Powell and Sara Steele [1996]Collecting Evaluation Data Direct Observation published for Program development and evaluation

20.Sui Generis [2006]Data Flow Diagram Process published under the process no CMPE202-5-Sui2 on September 29, 2006 san Jose State University.

21.Pavan Kumar Gadireddy [2007]Software Engineering – Concepts and Implementation Published in Centre for Information Technology and Engineering, ManonmaniamSundaranar University [2007]

22.Zapata, M and Asokan, N. (2002) Securing ad hoc routing protocols, in Proc. ACM Workshop Wireless Secur.

23.Kuladinith, K A. S. Timm-Giel, A.S. and Görg, C. (2004) Mobile ad-hoc communications in AEC industry, J. Inf. Technol. Const., vol. 9, pp. 313–323.

24.Stanoevska-Slabeva, K andHeitmann,M.(2003)Impact of mobile ad-hoc networks on the mobile value system, in Proc. 2nd Conf. m-Bus., Vienna, Austria.

25.Buttyan, L and Hubaux, J.P. (2007)Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press.

26.Al Agha, K.,Bertin, M.H., Dang,T.A.,Guitton., Minet, P., Val, T andViollet, J.B.,(2009) Which wireless technology for industrial wireless sensor networks? The development of OCARI technol, IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278.

27.Akbani, R.H., Patel, S and Jinwala, D.C.(2012) DoS attacks in mobile ad hoc networks: A survey, in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, pp. 535–541.

28.Dondi, D., Bertacchini, A., Brunelli, D.,Larcher, L and Benini, L.(2008)Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766.

29.Hu, Y., Perrig, A and Johnson, D.(2002)ARIADNE: A secure on-demand routing protocol for ad hoc networks, in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, pp. 12–23.

30. Lee, J.-S.(2008)A Petri net design of command filters for semiautonomous mobile sensor networks,IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841.

31. Liu, K., Deng, J.,Varshney, P.K andBalakrishnan, K.(2007)An acknowledgment-based approach for the detection of routing misbehaviour in MANETs,IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550.

32.Patwardhan, Parker, J., Joshi, A., Iorga, M andKarygiannis, T. (2005)Secure routing and intrusion detection in ad hoc networks, in Proc. 3rd Int. Conf.Pervasive Comput. Commun., pp. 191–199.

33.Rocha, J.G.,Goncalves, L.M., Rocha, P.F., Silva, M.P andLanceros- Mendez, S.(2010)Energy harvesting from piezoelectric materials fully integrated in footwear,IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819.

34.Singh, Maheshwari, M andKumar, N. (2011)Security and trust management in MANET, in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, pt. 3, pp. 384–387.

35.Tabesh and Frechette, L.G. (2010)A low-power standalone adaptive circuit for harvesting energy from a piezoelectric micropower generator,IEEETrans. Ind. Electron., vol. 57, no. 3, pp. 840–849.

36. Zhou, L and Haas, Z.Securing ad-hoc networks, IEEE Netw., vol. 13, no. 6, pp. 24–30.

37.Sun,(2004)Intrusion detection in mobile ad hoc networks, Ph.D. dissertation, Texas A&M Univ., College Station, TX.

38.Anantvalee T and Wu, J.(2008)A Survey on Intrusion Detection in Mobile Ad Hoc Networks, in Wireless/Mobile Security. New York: Springer-Verlag.

39.Sheltami, T., Al-Roubaiey, A.,Shakshuki, E andMahmoud, A.(2009)Video transmission enhancement in presence ofmisbehaving nodes inMANETs,Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282.

40.Marti, S., Giuli, T.J., Lai, K and Baker, M.(2000)Mitigating routing misbehaviour in mobile ad hoc networks, in Proc. 6th Annu. Int. Conf. MobileComput. Netw., Boston, MA, pp. 255 265.

41.Menezes, van Oorschot, P and Vanstone, S. (1996) Handbook of Applied Cryptography. Boca Raton, FL: CRC, T-37.