International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 11, November - 2014 | ISSN 2321-6905

International Journal of Science Engineering and Advance Technology

Securing Manets By Using An Intrusion Detection System (Eaack)

1 **Sri. M. Vamsi Krishna,** 2 **D.Jaya Prakash**
1,2Dept. of CSE, Chaitanya Institute of Science & Technology, Kakinada, AP, India

Abstract:
MANET arrangement may diverge depending on its application from a small static network that is extremely power inhibited to a large-scale, mobile, highly dynamic network. Every node works both as a transmitter and a receiver. Nodes converse directly with each other when they are both within the same communication range. Otherwise they depend on their neighbours to relay messages. Industrial remote access and control via wireless networks are flattering more and more popular these days. One of the chief advantages of wireless networks is its capability to permit data communication between different parties and still maintain their mobility. This communication is incomplete to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is further than the communication range of their own. MANET solves this problem by allowing intermediate nodes to rely data transmission. In this case detection should be focused as another part before an attacker can damage the structure of the system.

Keywords: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET).

Introduction:
EAACK exhibits higher malicious behaviour detection rates in definite conditions while does not greatly affect the network performances. MANET is becoming more and more extensively implemented in the industry. Nonetheless allowing for the fact that MANET is accepted among critical mission applications, network security is of vital importance. Regrettably the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For illustration because of the nodes lack of physical protection, malicious attackers can easily detain and compromise nodes to achieve attacks. In meticulous considering the fact those most routing protocols in MANETs imagine that every node in the network behaves cooperatively with other nodes and presumably not malicious attackers can easily compromise MANETs by inserting malicious or no cooperative nodes into the network. In addition because of MANET's distributed architecture and changing topology a traditional centralized monitoring method is no longer feasible in MANETs. In such case it is essential to develop an intrusion-detection system (IDS) specially designed for MANETs.

Related Work:
The requirement based approach is in recent times presented and is ideal for new environments such as MANETs. In specification-based detection the correct behaviours of critical objects are inattentive and crafted as security specifications which are compared to the actual behavior of the objects. Intrusions which usually cause an object to behave in an erroneous manner can be detected without exact knowledge about the nature of the Intrusions. at present specification-based detection has been applied to advantaged programs applications and several network protocols. Most of recent researches focused on providing preventative schemes to secure routing in MANETs. Intrusion detection is definite as the technique to identify "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". For MANETs, the general function of IDS is to detect misbehaviors by observing the networks traffic in a Mobile Ad hoc.

Literature Survey:

The paper presents the results of studies under taken routing misbehavior in MANETs Mobile Ad Hoc Networks. The node misbehaviors may be initiated due to the open structure and scarcely available battery-based energy and such routing misbehavior is caused by the selfish nodes that when processor contribute in the route discovery and preservation declines to forward the data packets. In the present studies it is proposed a novel scheme named 2ACK which provides an add-on technique for routing schemes that perceives the routing misbehavior and to overcomes their unpleasant effect. The main feature of 2ACK is to send two-hop acknowledgment packets in the opposite direction of the routing path

and to diminish additional routing overhead. The performance of the proposed scheme was analyzed and simulated and 95% packet delivery ratio was achieved when 40% misbehaving nodes were present in the MANETs. In this paper we propose a methodology for optimizing a solar harvester with maximum power point tracking for self-powered wireless sensor network (WSN) nodes.

Existing Model:

The open medium and remote distribution of MANET make it helpless to various types of attacks. For instance, due to the nodes' lack of physical protection, malicious attackers can easily confine and compromise nodes to achieve attacks. Moreover, as of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer possible in MANETs. Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes prepared with a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links whichever directly or indirectly. MANETs believe that every node in the network behaves considerately with other nodes and most probably not malicious, attackers can easily compromise MANETs by place in malicious nodes into the network.

Disadvantages:

Because of the limited battery power nature of MANETs such redundant transmission process can easily degrade the life span of the entire network. Watchdog scheme unsuccessful to notice malicious misbehaviors with the presence ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping. The idea of adopting a hybrid scheme in AACK significantly reduces the network overhead but still suffer that they fail to detect malicious nodes with the presence of false misbehavior report and fake acknowledgment packets.

Proposed Method:

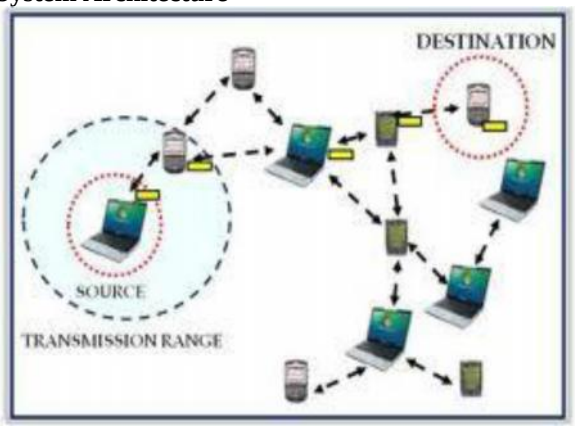
LeakDetector is that the destination node of a route builds up a virtual graph, which models the multipath from the source node to the destination node. Periodic traffic information enables the destination node to calculate the ratio of incoming and outgoing traffic corresponding to the multipath routing information for each participating node.

The destination node compares per route the incoming ratio with the outgoing ratio for each node participating. When the deviation is too large, the node is assumed to be malicious.

Advantages:

Our proposed Leakdetector *is* to detect colluding misbehaving nodes in the network.
Our solution comes with a low overhead and at no additional computational cost

System Architecture



Implementation:
Ids In Manet's:
Due to the restrictions of most MANET routing protocols nodes in MANETs suppose that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the prospects to achieve important impact on the network with just one or two compromised nodes. To address this problem, IDS should be added to improve the security level of MANETs. If MANET can detect the attackers as soon as they enter the network we will be able to completely abolish the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs and they are a great complement to existing proactive approaches.

Ack Implementation:
ACK is essentially an end to end acknowledgment scheme .It is a part of EAACK scheme aspiring to decrease the network overhead when no network misbehavior is detected. The basic flow is if Node A sends a packet p1 to destination Node D if the entire middle node is cooperative and effectively receives the request in the Node D. It will propel an ACK to the source Node A if ACK from the destination get deferred then it S-ACK process will be initialized.

ISSN 2321-6905

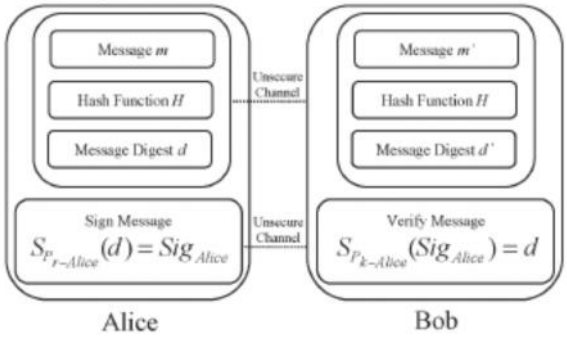
Secure Acknowledgment (S-ACK):

The purpose of initiating S-ACK mode is to detect misbehaving nodes in the existence of receiver collision or limited transmission power. In the S-ACK theory is to let every three successive nodes work in a group to perceive misbehaving nodes. For every three successive nodes in the route the third node is necessary to send an S-ACK acknowledgment packet to the first node.

Mra- Misbehavior Report Authentication:

The MRA method is considered to resolve the limitation of watchdog with respect to the false misbehavior report. In this source node verifies the vary route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

Digital Signature Validation:

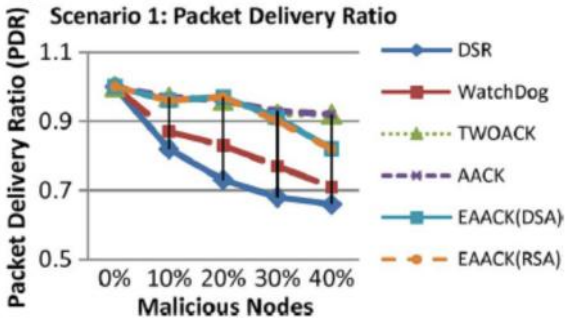


Thus it is tremendously significant to make sure that all acknowledgment packets in EAACK are genuine and untainted. Or else if the attackers are elegant enough to fake acknowledgment packets, all of the three methods will be vulnerable. In ACK, S-ACK and MRA are acknowledgment-based detection methods. They all depend on acknowledgment packets to detect misbehaviors in the network.

Leakdetector Implementation

The main idea of *LeakDetector* is that the destination node of a route builds up a virtual graph, which models the multipath from the source node to the destination node. Periodic traffic information (which can be piggybacked on the proactive routing messages) enables the destination node to calculate the ratio of incoming and outgoing traffic—corresponding to the multipath routing information—for each participating node. Using graph theory, traffic leaks are identified. In particular, the destination node compares per route the incoming ratio with the outgoing ratio for each node participating. When the deviation is too large, the node is assumed to be malicious

Experimental Results:



We examine that all acknowledgment-based IDSs carry out better than the Watchdog scheme. Our proposed scheme EAACK surpassed Watchdog's performance by 21% when there are 20% of malicious nodes in the network. From the results we bring to a close that acknowledgment-based schemes including TWOACK, AACK and EAACK are capable to detect misbehaviours with the presence of receiver collision and limited transmission power. However when the number of malicious nodes reaches 40%, our proposed scheme EAACK's performance is lower than those of TWOACK and AACK. We simplify it as a result of the introduction of MRA scheme when it takes too long to obtain an MRA acknowledgment from the destination node that the waiting time exceeds the predefined threshold.

Conclusion:

The mobility and scalability carry by wireless network made it probable in many applications. Among all the contemporary wireless networks,
Mobile Ad hoc NETwork (MANET) is one of the most imperative and unique applications. On the contrary to traditional network architecture, MANET does not necessitate a fixed network infrastructure as every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise they rely on their neighbours to relay messages. The self-configuring ability of nodes in MANET made it admired among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks.

References:

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.
[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.
[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.
[5] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "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, Jul. 2008.
[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.
[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.
[10] G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582, 2007.
[11] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.
[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.
[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile *ad-hoc* communications in AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323, 2004.
[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

Authors:

Sri. M. Vamsi krishna, well Known Author and excellent teacher Received M.Tech (AI &R), M.Tech (CS) from Andhra university is working as Professor and HOD, Department of CSE, Chaitanya Institute Science and Technology. He has 13 years of teaching & research experience. He has 20 publications of both national and international conferences /journals. His area of Interest includes AI, Computer Networks, information security, flavors of Unix Operating systems and other advances in computer Applications.

Mr. D. Jaya Prakash is a student of Chaitanya Institute of Science& Technology, Madhavapatnam, Kakinada
Presently he is pursuing his M.Tech. [Computer Science & Engineering] from this college and he received his M.C.A. from Dr.L.B. College of PG Studies, affiliated to Andhra University, Visakhapatnam in the year 1997. His area of interest includes Computer Networks, Advanced data structures and all current trends and techniques in Computer Science.