ISSN No. 0976-5697

Volume 4, No. 5, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Cross Layer Based Security in MANET

K.Suresh Babu
Research Scholar
School of Information Technology
JNT University Hyderabad
Hyderabad, India
Kare_suresh@yahoo.co.in

K.Chandrasekharaiah
Professor in CSE
School of Information Technology
JNT University Hyderabad
Hyderabd, India
chandra_sekharaiah@yahoo.com

Abstract : Mobile adhoc networks (MANETs) are prone to many security attacks and risks due to its characteristics such as mobility, lack of infrastructure and dynamic topology changes. The layered architectures are not in a position to adjust with the dynamics of the current wireless generation networks. Cross layer architecture will provide efficient solutions by providing interactions between different layers. In MANETs the cross layer techniques provide better solutions. In this paper, we try to study the existing cross layer techniques and propose a new cross layer based security in Mobile ad hoc networks.

I. INTRODUCTION

A. Mobile Ad hoc Networks (MANETs)

A mobile ad hoc network (MANET) is a kind of wireless ad hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which forms an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably [1]. These networks are characterized by dynamic network topology, lack of central administration and limited resources such as power and bandwidth [2]. Wireless ad-hoc networks consist of mobile nodes equipped with, among other components, a processor, some memory, a wireless radio, and a power source [3]. Wireless ad hoc network needs some special treatment as it intrinsically has its own special characteristics and some unavoidable limitations compared with wired networks [4].

The main feature of wireless ad hoc networks is its ability to allow a group of communications nodes to set up and maintain a network among themselves, without the support of a base station or a central controller. Many technological factors, such as cheaper hardware, smaller transceivers, and faster processors are increasing the interest in wireless ad hoc networks. Wireless ad hoc networks are useful for situations that require temporary networking capability, such as crisis response, conference meetings, sensor networks, military applications, home and offices networks, etc [5].

B. Security Threats

The security issues include the transmission of the data packets to the destination node by choosing an alternative optimum path and causing the minimum delays in the network transmission.[6] MANETs introduce various security risks due to their open communication medium, node mobility, lack of centralized security services, and lack of prior security association. In high-security MANETs, user authentication is critical in preventing unauthorized users from accessing or modifying network resources [7]. An adhoc network can be attacked from any direction at any node which is different from the fixed hardwired networks with physical protection at firewall and gateways. Altogether it denotes that every node should be equipped to meet an attacker directly or indirectly. Malicious attack can be initiated from both inside and outside of the network. Tracking a specific node is difficult in large adhoc networks and hence, it is more dangerous and much difficult to detect the attacks from an affected node. Altogether it denotes that every node should be prepared to work in a way that it should not trust on any node immediately. Distributed architecture should be applied in order to achieve high availability. This is because if the central entity is used in the security solution, it causes serious attack on the entire network when the centralized entity gets affected [8].

C. Attacks on MANETs

Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service

The absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network [9]

D. Security Challenges in MANETs

People have practiced security for a long time. In the past, security services were considered only after the network service was totally designed.[23] These adhoc approaches turn out to be unsatisfactory. Hence to avoid such pitfalls, consider the security as integrated part of the System itself. Based on the analysis of the objectives from

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 25-26 March 2013
Organized by
Vignan University, India

the customer side, operator side and public community, the main security objectives for the System are Confidentiality, Data Integrity, Accountability & Availability. The nature of MANET makes it vulnerable to attacks. Challenges in MANET securities are discussed briefly

- **Confidentiality:** should preserve certain information which is not to be opened to unauthorized parties.
- **Integrity:** The receiver should believe that the transmitted message is genuine and is never be corrupted.
- **Authentication:** Enables a node to defend the characteristics of the peer node it is communicating, without which an attacker would duplicate a node.
- **Access control** prevents unauthorized use of network services and system resources. Access control is tied to authentication attributes.
- **Availability:** should withstand survivability regardless of Denial-of-Service (DOS) attacks like in physical and media access control layer attacker uses jamming techniques for hinder with communication on physical channel. [10]

E. Cross Layer Techniques

Cross-layer design breaks away from traditional network design, where each layer of the protocol stack operates independently and exchanges information with adjacent layers only through a narrow interface. In the cross-layer approach information is exchanged between non-adjacent layers of the protocol stack, and end-to-end performance is optimized by adapting each layer against this information Cross-layering is not the simple replacement of a layered architecture, nor is it the simple combination of layered functionality: instead it breaks the boundaries between information abstractions to improve end-to-end transportation. One obvious shortcoming of the strict layering is the lack of information sharing between protocol layers. This hampers optimal performance of the networks, since shared layer information is the prerequisite for many forms of performance optimization. On the other hand, cross-layer systems shift the research landscape away from optimizing the performance of individual layers, and instead treat optimization as a problem for the entire stack. The technique consists of taking into account information available from different levels, not necessarily adjacent, in order to create a system much more sensitive to its environment, load and usage.

Cross-layering can tackle the traffic in better manner on ad hoc networks by sharing information from different layers. Moreover, information collected at a particular layer (e.g., a route failure) can be exploited by different layers to tune the protocol behavior [11]. Existing proposals try to improve caching performance in a MANET environment, but they either focus on layered protocol based solutions, or do not exploit the benefits of cross layer design for cooperative caching [12]. Cross layer solutions reduce overhead and should thus be investigated for use in military tactical networks where bandwidth is the limiting factor [13]. One of the main advantages of the cross-layer architecture is to make protocols aware of the current state of the network from the point of view of the local node. The advantages of the Mobile MAN cross layer architecture with respect to the legacy one are also confirmed by the analysis of the quality of service experienced by the applications. [14] Cross layer design approach can be used to improve the overall performance of multihop wireless networks such as wireless sensor networks (WSN), mobile ad hoc networks (MANET), and wireless mesh networks (WMN) [15]. The cross-layer design approach is the most relevant concept in mobile ad hoc networks which is adopted to solve several open issues. It aims to overcome ad hoc networks performance problems by allowing protocols belonging to different layers to cooperate and share network status information while still maintaining separated layers [16].

II. RELATED WORK

A.Rajaram et al [8] have developed a trust based security protocol based on a cross-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, we provide link-layer security using the CBC-X mode of authentication and encryption.

John Felix Charles Joseph et al [17] have proposed CARRADS, a computationally efficient methodology for adapting the intrusion detection model at real-time. The adaptation process consists of two major stages. In the first stage, the main task is to identify occurrence of new patterns in the routing control traffic and prioritize them based on their information content. The second stage of adaptation is to incrementally update the detection model using the new patterns with minimum computational overhead. CARRADS uses SVM algorithm for its superior detection abilities.

Arjun P. Athreya et al [18] have proposed a cross-layer strategy for secure multi-path routing in MANETs. The routing decisions made at the network layer depend on feedback and inputs from the lower physical and link layers. Security is built into this routing mechanism and path selection is based on forwarding behaviors of nodes in the network and link quality of each hop in a path. We show that with mobile nodes, cross-layer strategy via information sharing from lower layers helps in achieving reliability in routing and path selection.

Min Shao et al [19] have proposed a cross-layer dropping attack against video streaming. We first identify a general IP layer dropping attack and then reveal its destructive impact by leveraging the application layer information (e.g., video streaming). We also propose several possible solutions to address the dropping attacks. Due to the unique characteristics of this attack, as long as malicious nodes exist, the network will suffer from this dropping attack.

Abderrezak Rachedi et al [20] have proposed a new cross-layer approach based on physical, MAC, and routing layers for a monitoring mechanism. A new analytical model

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 25-26 March 2013
Organized by
Vignan University, India

is proposed to illustrate the parameters' effect on these different layers. The impact of the signal to noise ratio (SNR) and the distance between monitor and monitored nodes are clearly introduced. Moreover, the difference between the carrier sense, the interference range, and the transmission range is taken into account in our model. The proposed model improves the evaluation of the nodes' cooperation and reduces the risk of having any false positive rate.

III. PROBLEM IDENTIFICATION & PROPOSED SOLUTION

In CARRADS [17], routing based misbehaviors are detected based on SVM based training. But it considers only abnormality in routing. Moreover, it does not provide any authentication mechanism for validating the reports. In [18], cross-layer approach is used only for establishing multipath routing. [20] provides a cross-layer monitoring process. But it does not provide any authentication mechanism for validating the reports. Also no suitable mechanism for selecting the monitoring nodes is also discussed. So we need to design a cross-layer based security solution which provides security for attacks against all the layers which should also authenticate and protect the messages exchanged. In this proposal, we propose a cross layer based security in mobile ad hoc networks. It consists of monitor nodes which are used to monitor their neighbors. Initially, a mechanism for monitor node selection is designed such that the monitoring nodes are stable and should cover the entire network. The monitor node selection is based on the metrics from the two layers. The physical layer estimates link stability and residual energy and the node degree is obtained from routing layer. After selecting a monitor node, it estimates the trust value for each of its neighboring node. The trust value is estimated as a ratio of the number of packets observed by the monitor node divided by the total number of packets sent by a monitor node and well-received by a monitored node [20]. The trust value is piggybacked in the route request (RREQ) packets. When the source S wants to send data to the destination D, it sends route request (RREQ) packets towards D. The RREQ can be protected with the hop-by hop authentication. In subsequent hops, the intermediate nodes create a Message Authentication Code (MAC) value and encrypt it using a shared symmetric key, They append their ID with encrypted payload from previous node until the destination D reaches [18]. On receiving the message, D decrypts the value in the reverse order of the ID's recorded and verifies the value sent by S with the decrypted version of the value sent by all intermediate nodes. In D, if any intermediate node fails authentication, then the trust value is decremented. Then the updated trust values are sent to S, through route reply (RREP) packets. The computed trust values of the nodes are passed to routing layer and the MAC layer. Routing layer selects the high trusted nodes for routing. The media access control (MAC) grants more access time for high trusted nodes.

IV. CONCLUSION AND FUTURE SCOPE

In this paper the cross layered techniques for MANETs have been studied. From the study it has been found that there are some security flaws in the existing techniques. It proposes a new cross layer based security for MANETs by utilizing the information from physical, data link and network layers. As a future work it is proposed to implement this proposal in NS2 simulation environment.

V. REFERENCES

[1] K.Suresh Babu, K.ChandraSekharaiah, "Issues Related to Routing and Security in Mobile Ad-Hoc Networks", January 2009, CI-4.7, International Conference on Systemics, Cybernetics and Informatics ICSCI-2009, January 07-10 2009.

[2] Hwee Xian TAN and Winston K. G. SEAH, "Dynamic Topology Control to Reduce Interference in MANETs" Proc. of the 2nd Int'l Conf. on Mobile …, 2005 - comp.nus.edu.sg

[3] Pascal von Rickenbach, Stefan Schmid, Roger Wattenhofer, Aaron Zollinger, "A Robust Interference Model for Wireless Ad-Hoc Networks" Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International Digital Object Identifier: 10.1109/IPDPS.2005.65 Publication Year: 2005 Cited by: 4 IEEE Conferences

[4] Kousha Moaveni-Nejad, Xiang-Yang Li, "Low-Interference Topology Control for Wireless Ad Hoc Networks" Ad Hoc & Sensor Wireless Networks, 2005 – Citeseer

[5] R. P. Ramos, M. Geandre R.ego, Tarciana Lopes, R. Baldini Filho and C. de Almeida, "Interference Evaluation in CDMA Ad Hoc Networks" Telecommunications Symposium, 2006 International Digital Object Identifier: 10.1109/ITS.2006.4433411 Publication Year: 2006 , Page(s): 967 - 970 IEEE Conferences

[6] Tanu Preet Singh, Manmeet Kaur, Vishal Sharma, "Automated Recovery Based Power Awareness (ARPA) Algorithm for MANETs" 2011 International Conference on Circuits, System and Simulation IPCSIT vol.7 (2011) © (2011)

[7] K.K.Lakshmi Narayanan, A.Fidal Castro, "High Security for Manet Using Authentication and Intrusion Detection with Data Fusion" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518

[8] A.Rajaram, Dr.S.Palaniswami, "A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 1, 2009

[9] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey" The, 2007 - cs.umbc.edu

[10] S.Gopinath, Dr.S.Nirmala & N.Sureshkumar, " Misbehavior Detection : A New Approach for MANET" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.993-997

[11] Jyoti Jain, Mehajabeen Fatima, Dr. Roopam Gupta, Dr. .K.Bandhopadhyay," Overview and challenges of routing protocol and MAC layer in Mobile Ad hoc network" Journal of Theoretical and Applied Information Technology© 2005 - 2009 JATIT.

[12] Mieso K. Denko and Jun Tian, "Cross-Layer Design for Cooperative Caching in Mobile Ad Hoc Networks" Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE Digital Object Identifier: 10.1109/ccnc08.2007.90 Publication Year: 2008 , Page(s): 375 - 380 Cited by: 2 IEEE Conference Publications

[13] Anders Fongen, " Certificate Validation In Military Manet Based on overlay network of XKMS proxies" Military Communications Conference, 2008. MILCOM 2008. IEEE Digital Object Identifier: 10.1109/MILCOM.2008.4753213

Publication Year: 2008 , Page(s): 1 - 8 IEEE Conference Publications

[14] Eleonora Borgia, Marco Conti, and Franca Delmastro, MobileMAN: Design, Integration, and Experimentation of Cross-Layer Mobile Multihop Ad Hoc Networks" Communications Magazine, IEEE Volume: 44 , Issue: 7 Digital Object Identifier: 10.1109/MCOM.2006.1668386 Publication Year: 2006 , Page(s): 80 - 85 Cited by: 1 IEEE Journals & Magazines

[15] Amardeep Singh, Gurjeet Singh, "Security in Multi-hop Wireless Networks" IJCST Vol. 2, Iss ue 2, June 2011 International Journal of Computer Science and Technology ISSN : 2229 - 4333 (P r i n t) | ISSN : 0976 - 8491

[16] Noureddine Kettaf, Hafid Abouaissa, Thang Vuduong† and Pascal Lorenz, "A Cross layer Admission Control On-demand Routing Protocol for QoS Applications" IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.9B, September 2006

[17] John Felix Charles Joseph , Amitabha Das b, Bu-Sung Lee, Boon-Chong Seet , "CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS" Computer Networks, 2010 – Elsevier

[18] Arjun P. Athreya and Patrick Tague," Towards Secure Multi-path Routing for Wireless Mobile Ad-Hoc Networks: A Cross-layer Strategy" Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference on Digital Object Identifier: 10.1109/SAHCN.2011.5984886 Publication Year: 2011 , Page(s): 146 - 148 IEEE Conference Publications

[19] Min Shao, Sencun Zhu, Guohong Cao, Tom La Porta and Prasant Mohapatra, "A Cross-layer Dropping Attack in Video Streaming over Ad Hoc Networks" Proceedings of the 4th …, 2008 - dl.acm.org

[20] Abderrezak Rachedi and Abderrahim Benslimane, "Toward a cross-layer monitoring process for mobile ad hoc networks" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks. (2008) Published online in Wiley InterScience (www.interscience.wiley.com) DOI: 10.1002/sec.72

[21] K.P.Manikandan, R.Satyaprasad, K.Rajasekharara, "A Cross Layered Architecture and Its Proposed Security Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3), 2011, 1007-1011

[22] Wei Wei and Avideh Zakhor, "Interference Aware Multi-Path Selection for Video Streaming in Wireless Ad Hoc Networks" Circuits and Systems for Video Technology, IEEE Transactions on Volume: 19, Issue: 2 Digital Object Identifier: 10.1109/TCSVT.2008.2009242 Publication Year: 2009 , Page(s): 165 - 178 Cited by: 5 IEEE Journals.

[23] K.Suresh Babu, K.ChandraSekharaiah, "System Security: A Survey", National Conference Proc. RESPOGRAF, ASTRA, 2008.