Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A New Fuzzy Based Secured Routing for Wireless Sensor Network

Dr. Gadiparthi Manjunath
Asst.Prof, Department of IT & SC
AAIT, Addis Ababa University
Addis Ababa, Ethiopia

***Abstract** - WSN or Wireless Sensor Network is implemented across wide area of applications, including agriculture, defence and so on. A sensor network is a wireless network of the sensors deployed across a wide field, where the objective is to transmit data from the sensor nodes to a central server. As the range of the sensors is very low, and the area of deployment is quite wide, direct data diffusion from sensor to the server is not possible. Therefore multipath routing is adopted in such networks which enable the source sensors to transmit data either through intermediate sensors or special nodes called sink nodes. Due to wireless transmission, data is vulnerable to various kinds of attack. Due to low energy of the nodes, a centralized key management system for security is not feasible in such a network. Therefore we present a unique solution for sensor network based on fuzzy keys generated by the nodes based on various network parameters of the nodes. WNS sessions (communication stream between source and the server or sink) are generally short and busty which requires the security extension to be designed in such a manner that the keys are short lived and refreshed frequently in order to make it impossible for intruder to hack any data. This key is further combined with a device level password for authentication and digital content encryption. As the state of the nodes differs almost in every session and sometimes in the middle of a session, hacking such key is theoretically "impossible" as key refresh time is minimum here. The proposed technique is simulated with OMNET++ environment. Result shows significant prove of real time adaptability of the technique.*

***Keywords**: Fuzzy, WSN, QOS, Multipath, Security, Key Management.*

I. INTRODUCTION

Wireless Sensor network is an infrastructure less network where source sensor diffuses the data to sink. These data are sensed parameters like temperature, humidity or video streams as generated by surveillance sensors. Data and packets through intermediate nodes. The directed set of intermediate nodes through with a source diffuses the data to destination sink is known as a route. The process of route building can be both proactive and reactive. Due to variability in network conditions, a preformed route may guarantee quality of service. The Routing steps are more clearly explained in [1], which has explained the concept with respect to mobile adhoc network that is adopted here in WSN. Now let us analyze the security loopholes of WSN and possible attacks by considering a sample topology as demonstrated in Fig. 1 which comprises of both authenticated and non authenticated nodes.

It is clear that control messages like RREQ and hello packets are received by all the nodes, including the authenticated nodes which lead to their inclusion in the path as shown in Fig. 4. Due to variability in node conditions like energy and power loss in the network, in a single session there may have to form more than one path from source to destination. Thus the observation leads to following criteria for secured WSN environment.

a) Nodes must be pre-authenticated and that that each node must know the authenticity of all the other nodes in their neighbourhood

b) RREQ packets must be encrypted so that only authenticated nodes can read the header and therefore only authenticated nodes can include them in the path.

c) Key must be refreshed frequently in order to avoid guessing. This is because wireless impersonating nodes will receive many messages in the wireless environment that leads to significant database for guessing the key.

d) The initial authentication must be fast for fast route building process

II. LITERATURE SURVEY

Charles Perkins [1] introduced the fundamental concept of MANET and AODV routing that is adopted in WSN. Hao Yang et al. [2] identifies the basic problem of MANET for offering a security to the traffic which acts as basic problem identification for the current work. Zheng Ming Shen [3] claims that QOS and Security are two integral part of MANET and security extensions must not affect the desired QOS of MANET. Papadimitratos [4] models a novel framework for demonstrating malicious disruption in data transmission and simulates secured message transmission over secured single path. The understanding of more fundamental problems for offering better security solutions for MANET is attributed by factors like change in topology, co-operative nature of the routing which both violates the basic principal of security systems[5]. Most significant protocols in wireless network that desire strong security protocol to be incorporated in order to prevent impersonation is explained by Pradip M.[6]. In order to bring network monitoring into play in the dynamic MANET architecture, intermediate nodes must be given the responsibility of detecting attacks in a route. This scheme is presented by Kathirvel [7] where a node is given the responsibility of forwarding as well as monitoring or "umpiring". [8] Proposes a secured routing protocol. The key distribution technique for MANET was proposed long back in 1999 by Lidong Zhou [9]. But the system model is based on configuring special key distributing nodes called servers. MANET is widely accepted due to its decentralized nature. Therefore public key cryptography with centralized key distribution cannot be considered as the best scheme for MANET security which is further strengthened by an alternative approach[10, 11].

III. PROPOSED WORK

There may be three types of nodes possible in the topology 1) Valid Nodes, 2) Nodes which are part of the authenticated network but not authenticated for participating in current data transmission, 3) Nodes which are unauthenticated for the network. Most of the security extensions consider only node type 3 as threat. Such nodes are eliminated through an initial key exchange which is derived from a preloaded hash table. The second category of nodes is more challenging with respect to the network security perspective. In this work, the treat elimination of category 2 nodes is achieved through a second category of key that we propose in this work. This is called a QOS Fuzzy key. This is generated from the QOS parameters in a node. The considered parameters are Residual Energy of a Node, Average Received Power, Relative Mobility, Residual Bandwidth, Average Observed Delay, Average MAC queue size. The key is generated from a binary sequence of the state of the parameters, resolved through Fuzzy as High, Low and Medium. The generated key is used to encrypt the packet header of both data and control packet. As the state of the impersonating nodes varies very rapidly, the key of the node also varies, which eliminates it from the routing entity. Further in order to achieve the more security a multipath approach is adopted which prevents the entire data being exposed to the intermediate nodes.

IV. METHODOLOGY

We divide the overall system into following sub-problem and present the security extension in each stage.

a) Initial Authentication of the Nodes: In this work we consider the deposition of a Hash table in each valid nodes belonging to the network. The hash table contains several hash values in a matrix format.

The hash table is generated from a hash function which converts the set of {node ID range, IP address Subnet mask, MAC address range} to hash function and uses a discrete random function for generating and randomizing the same. If it is assumed that all the valid nodes of the network are preloaded with the proposed protocol suite then each node with come on board with the hash values.

Initially as nodes exchange hello message. In the hello message, the node IDs and hop fields are appended. The initial hello message is incorporated with a cipher generated from user level password which is assumed to have been distributed amongst the nodes which are authenticated for transmission. This cipher text is encrypted with a random hash from the hash table. Once a node receives the message, it tries to decode the message with all possible combination of hashes from the table and matching the cipher text for each instance. This is time consuming and consumes a lot of computation cycle. To reduce the computation cycle, the hash value index is selected from a hash selection function which takes the common user password as input.

This step reduces the search complexity to only single index search. Now the authenticated nodes can easily decipher the hello message and build the node ID.

Type 2 of nodes cannot extract the actual hash because it does not know the initial password. Therefore it needs two steps for decoding. One search through all the hash values to select a particular hash. Even if it tracks the hash, it is not aware of the user level common password. Hence it cannot generate a valid hello message to embed itself in the routing table of the other nodes. As a worst case scenario, if the imposter somehow knows the initial password, it gets itself authenticated initially. Hence extreme caution must be adopted for this key exchange amongst the user. Nodes 3 are easily eliminated from the initial routing table.

b) RREQ transmission phase and Route Building

As First stage eliminates the node 3 type of node, the objective of the protocol is to eliminate the participation of node type 2 and authenticate and include only node 1. Most trusted end to end secured communication is carried out with the help of public key cryptography where each node maintains two pairs of keys: a public key and the private key. Transmitter encrypts the message with the public key and the receiver decrypts the message with the private key. As WSN routing must include intermediate node, the intermediate nodes must know the public key. As it is understood from our proposal that each of these type 2 nodes have a valid hash table and know the possible public key. We develop a fuzzy inference system with following outputs VERY LOW, LOW, MEDIUM, HIGH, and VERY HIGH. Each of the matrices are associated with three type of input LOW, MEDIUM, HIGH. Each authenticated nodes are loaded with a hash generation method that takes input as 7 byte characters generated from the input fuzzy set. LLHMML sequence is generated for low bandwidth, low delay, high energy, medium queue size, medium relative mobility and low power loss. The source node encrypts the RREQ packet with the generated hash from the desired set of values. As RREQ packet is received by a node, the node generates the hash from its own state of information and decrypts the RREQ. If the RREQ is decrypted successfully, a node forwards the packet. For type 3 node, decrypting the control message is widely difficult and thus it does not know the basic information of the message passing.

Selected nodes when participate in the routing, the packet headers are encrypted with the hash key generated from the initial structure, where as the data is encrypted with the public key of the network which is a randomly selected initial hash value.

c) Effect of impersonating on the QOS state and the Fuzzy Key

If a node in the route decides to impersonate, its energy goes down very fast, queue size decreases, node suffer more power loss which changes its QOS state very fast. Therefore further packet header which are to be routed through this nodes are not routed which shoots up an route error packet that leads to route error.

V. RESULTS

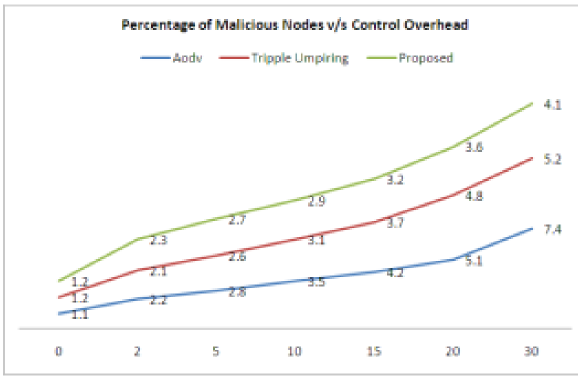

Fig. 1. (a) Percentage of Malicious Nodes v/ control overhead and

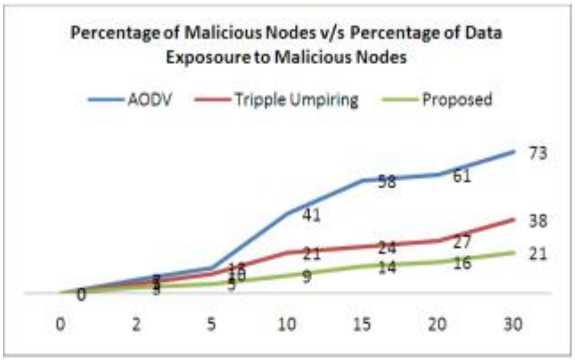

Fig. 1 (b) Percentage of Malicious Node v/s Percentage of Data Exposure to Malicious Nodes

Fig. 1. (a) Shows that as the density of malicious nodes vary, control overhead also increase. This is due to route refreshment and delay and pdr sensitivity of the network. Control Overhead is least in the proposed technique due to the presence of multiple paths. Hence RERR are not generated immediately and the transmission continues with existing paths. Fig. 1. (b) is an interesting finding. Without any monitoring algorithm, data being exposed to malicious nodes are very high. Whether they are being decrypted or not is not the question here. The main observation is that triple umpiring significantly reduces the overall exposure. This is further improved by the proposed technique.

VI. CONCLUSION

There are various monitoring and security extension proposed over the years in wireless sensor network. MAC layer embedded security extension or WEP is most widely adopted of these extensions. But the WEP security extension bargains huge energy which is a drawback. Therefore alternative key management techniques for WSN are in demand. Mostly the key management and QOS are considered as related entities. But no work has presented a QOS offering through the key management itself. Further Intrusion detection through network parameter monitoring is considered as a separate entity. In this paper we have shown that by generating the key from the QOS state of a node, one can not only extend the security of the network also at the same time guarantee QOS. The adaptation of Multipath routing further strengthens the security by minimizing the data exposure to malicious nodes. The system can be further improved by a hash function which not only can translate the Fuzzy Equal-Output to a key but also conditions like Greater-Than-Equal-To functions to keys. As the observation shows that network performance vastly degrades with attacks, nodes that provide good or better QOS must be incorporated. There bound to be performance variations if malicious nodes are present.

REFERENCES

[1] Perkins, C., Royer, E.: Ad Hoc On-Demand Distance Vector Routing. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps. (1999)

[2] Shen, Z. M., Thomas, J. P.: Security and QoS Self-Optimization in Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing,Vol. 7, Issue 9 (2008)

[3] Papadimitratos, P., Haas, Z. J.: Secure data communication in mobile ad hoc networks. IEEE Journal on Selected Areas in Communication, Vol. 24, Issue (2006)

[4] Monica, Kumar, M., Rishi, R.: Security Aspects in Mobile Ad Hoc Network (WSNs): Technical Review. International Journal of Computer Applications, Vol. 12, No.2 (2010)

[5] Pradip, M., Jawandhiya, P. M.: A Survey of Mobile Ad Hoc Network Attacks. International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, (2010)

[6] Kathirvel, A., Srinivasan, R.: Triple Umpire System for Security of Mobile Ad Hoc Networks. International Journal of Network Management (2010)

[7] Papadimitratos, P., Haas, Z. J.: Secure Routing for Mobile Ad hoc Networks. In: Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (2002)

[8] Asokan, N., Ginzboorg, P.: Key Agreement in Ad Hoc Networks. Computer Communications, 23 (17), pp. 1627-1637(2000)

[9] Zhou, L., Haas, Z. J.: Securing Ad Hoc Networks. IEEE Network, special issue on network security(1999) .

[10] Selvan, G. S. R. E., Sivagurunathan, S., Subathra, P., Nidhya, S. D.: Mobile Ad Hoc Network Security- A Cluster based Approach. Journal of Computers, Vol.20, No.3 (2009)

[11] Manikandan, J., Vijayaragavan, S.: Multihost ad-hoc network with the clustered Security networks. International Journal of Engineering Science and Technology, Vol. 2(3) (2010)