Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200159

Device Authentication and Secure Routing in MANET for Internet of Things

Kirubadevi Thiyagarajan[a,1], Ramamoorthy S[b] , Neelavathy Pari S [c] and Rajakumar P S [d]

[a] *Dept of CSE, Dr.M.G.R Educational and Research Institute, Chennai*
[b] *Professor, Dr.M.G.R Educational and Research Institute, Chennai*
[c] *Assistant Professor, Dept of CSE, Madras Institute of Technology, Chennai*
[d] *Professor, dept of CSE, Dr.M.G.R Educational and Research Institute ,Chennai*

Abstract. In the next generation of communication mobile adhoc network (MANET) will play a major role in Internet of Things (IoT).MANET can be defined as a network among a group of nodes with no infrastructure. Internet of Things is the composition of a variety of networks like Wi-Fi, ZigBee, Wireless Sensor Networks (WSNs).MANETs, and Radio Frequency Identifier (RFID). There is a need for the compatibility of MANET with IoT for the deployment of smart infrastructure. Authenticity and security in communication between devices are essential for the realization of IoT with MANET. Authentication and providing security in MANET are always challenging due to its mobility in nature. Devices in IoT are usually resource constrained in energy, memory, computation and bandwidth. Therefore, it is difficult for each node to authenticate all the devices in the network. In this paper, an authentication scheme is proposed without any third party provider to distinguish the authorized and unauthorized devices. This authentication consists of two level process; in the 1st level mutual devices are authenticated, and in the 2nd level secure data routing between the devices is carried out. Mutual authentication is performed by Clustering based on keys and unique identities and by the cluster heads interpreting for secure routing. This scheme ensures the early measure of authenticity for the message requested enters into the IoT networks and disagreement against attacks.

Keywords: IoT, MANET, Clustering, cluster head, consistency, malicious device, Authentication, Secure routing.

1. Introduction

The Internet of Things(IoT) is the association of different devices (both physical and logical) like vehicles, automation objects, embedded software, sensors, connectivity and actuators. MANET is a dispersed group of wireless nodes that can work without the existence of stable network infrastructure. In this network, the nodes are open to travel erratically at any specified time. The movement of nodes determines network topology and interconnections among the nodes can transform quickly randomly. Therefore, nodes need to be coordinated for multi-hop interactions. Security is a major concern in MANET. Because of its uncovered connectivity, resource restrictions, without bounded physical guard of the mobile nodes [1]. Thus, MANETs are more inclined to security threats. Authentication plays an important role in security of the network. Currently, there are many existing secure

[1]Kirubadevi Thiyagarajan, Dept of CSE, Dr. M.G.R Educational and Research Institute, Chennai; Email id: kirubadevi.t@drmgrdu.ac.in

solutions by a secure third party security association whereas in the proposed model clustering techniques are applied for authentication. A cluster based IoT MANET is used for the behavior-based framework for secure communication. Since the environment is open without any infrastructure any intruder can send fake messages thus creating Denial-of-Service attack. This paper discusses a device authentication scheme that supports both direct and indirect Device-to-Device (D2D) communication [2]. The following Section 2 reviews the research in the area of node authentication and secure routing in MANET and WSN. Proposed System is described in Section 3. Section 4 includes network model and Section 5 discusses the Performance Valuation followed by conclusions in Section 6.

2. Literature Survey

Aluvala, Srinivas,et.al proposed a novel mechanism of implementing ones complement and cryptographic mechanism for secure routing. The idea achieves minimum computational overhead whereas the performance metrics like jitter,throughput,packet delivery,etc need to be analyzed and this concept was the motivation for the proposed technique [3].Cluster based Authentication Scheme (CBAS) method was developed by C. Sivaranjani Devi and S.A. Arunmozhi used secret key indirectly passed with zero knowledge protocol (ZKP) between the nodes by the master node which overcomes the drawback of SPIN.The master node destroys the intermediate node for security [4].In BAS,cluster head generates the master key. If the masterkey is compromised it does not affect the network resisting from outside nodes and stop producing the keys for further communication but on the whole it lacks inside security to enhance the network performance. An authentication mechanism to secure AODV protocol was designed by Preet.et.al., which focused to differentiate unauthorized user to authorized one using the principle of prime factorization [5]. This process may suffer from RREQ flooding which may affect the secure routing and degrade the performance of the network. A light weight authentication BAS(Biphase Authentication Scheme) was proposed by Riaz, Rabia, et al.to authorize nodes entering the network and resist against denial of service attacks [6].There is a huge scope to improve the network performance and various non-deterministic factors like distance,energyetc. Rizvi,Sanam Shah and Tae-Sun Chung insisted on the disabilities of SPIN protocol [7]. Any compromised node in the network cannot be detected using SPIN and it is not suitable for large networks. A new node wishing to enter the network sends request to any node in the network [8],it forwards the request to KDC for authentication sake but the new node keeps flooding the request to the node thus degrading the performance and prone to DoS attacks [9]. S. Aruna and A. Subramani developed a metric based clustering that includes weight based clustering algorithm, weight based adaptive clustering and many more. Based on the performance, clustering seems to yield good results and lacks in addressing network performance issues.Xiao, Debao, Meijuan Wei, and Ying Zhou., highlighted the concept of SPIN which uses two level authentication scheme SNEP and TESLA [10]. It provides security using third party providers which uses KDC to generate keys for communication [11]. But it generates the secret key through the base station because

of which time, energy consumption and other performance metrics of the network is more and that proves to be a drawback in the protocols.

3. Proposed System

The proposed work is to perform authentication and secure routing in the IoT MANET. The initial step is clustering to elect the cluster head and to accomplish secure data transmission between devices. Clustering involves the following steps: Formation of cluster and selection of cluster head, Cluster is formed on the proximity of the devices. Each device will calculate the weightage based on the various parameters like $W_n = (x*E_n) + (y*D_n) + (z*d_n)$ *Where* W_n *= Weightage for a device n,* E_n= Energy level in the device n , D_n= Distance from the neighbor device n, d_n= Degree difference of device n ,where x,*y,z* are the coefficients. The device with a maximum weightage value will be nominated as cluster head. The cluster head will keep track of the other devices in the network maintaining a routing table with all parameters of other devices, such as IP address Cluster formation is carried out after electing the cluster head (CH). The CH head will inform about it to all other neighboring devices and will receive in turn a response "Willing to join in the cluster". Based on the responses CH will form the cluster and the device which receives responses from more than one CH will be considered as gateway device. Cluster head maintain a table in which device ID and its IP address and ones complement of the devices in the network are updated. .The secure routing algorithm is described below

3.1 Algorithm

Initialize: Ch-cluster head, n – new node
Step 1: n is the node which enters in to the network
calculate ones complement of IP address of n.
Step 2: Update the IP address of any node n in the cluster table.
Step3: Check for the efficient device by calculating the weights of each device. Devices exchange the weights and the device with the maximum weight is chosen as the "Cluster head", ch.
Step 4: (if weight(ch>n)) then n is replaced as new cluster head
Else ch remains as cluster head after certain period of time.
Step 5 : Data transmission- Secure routing
$S_{5.1}$→Sender IP address XORed with Destination IP Address= z
$S_{5.2}$→Route req(RReq) is send to the neighbor nodes from Sender{RReq is encrypted using public key}
$S_{5.3}$→As devices receive RReq, neighbor nodes verify IP address by adding ones complement to check the result is all 1's and forwards to destination.(performed using the ch table)
$S_{5.4}$→All neighbor nodes can verify IPaddress, but only destination node can decrypt theRReq message using its private key
$S_{5.5}$→$x=c_e(\text{mod } n)$ is used to generate plain text again.
$S_{5.6}$ →If z XOR Destination IP address gives source IP address. If IPs matched then

decrypt the message. Else "warning message is sent to all neighboring nodes in the network and IP address is blacklisted".

4. Network Model

Consider an IoT network of 13 wireless devices and a router which is in turn connected to base station. Cluster based topology is used for network formation.The power consumed in a device is the summation of power in the acquisition and processing the signals and transmitting and receiving them. Devices are represented in the form of motes. Each device transmit and accept messages with16.15 μJ/byte energy and 12.15 μJ/byte energy respectively. The power consumption varies with the distance of the devices (number of hops required). Cluster head node takes0.57 μJ energy to obtain encryption key by using symmetric key algorithm. Energy consumption of each device is calculated by,

$P_{Tx} = (T_x * b1) * H$ (1)

Where P_{Tx}- Transmitting power, P_{Rx}- Receiving power, P_{Kx} . Key generation power b1- the number of bytes sent by each CH, H- the number of hops used to send message between S to D. (sending and receiving devices)

$P_{Rx} = (R_x * b2)$ (2)

Here b2 is the number of bytes received in network.

$P_{Kx} = (K_x * e)$ (3)

Here e is the number of times encryption keys are generated by authenticator nodes .

P_{Tot} total power consumed is calculated as, $P_{Tot} = P_{Tx} + P_{Rx} + P_{Kx}$ (4)

Total messages sent and received gives the total messages communicated within the network, which will be calculated as, $M_{Tot} = M_{Sx} + M_{Rx}$ (5)

The sum of sent and received messages gives the total number of messages used for successful communication in the network. By applying the above equations the performance evaluation can be calculated as described above.

5. Performance Evaluation

The proposed scheme performance is evaluated for various parameters like power consumption, packets transmission quotient (packets sent/packets received) and was compared to existing schemes SPIN and BAS network model.

5.1Power Consumption.

The Energy consumption denotes the power consumption. BAS model derives authentication of the node is verified by the authenticator node. This will incur in more utilization of energy and hence network traffic increases. In the SPIN model, any new node is an adversary node. It sends request to CH. The CH communicates with other CH through multi hop wireless communication. In the proposed scheme, Cluster head is chosen as per the weight of individual devices. The CH is considered as authenticator. Any communication between devices is done through CH.

The number of transmitted messages in the network and the Cluster Heads involved in the communication differentiates total power consumption. The results are derived using Cooja Simulator. The transmission power of the proposed model is significantly

less when compared to the power used by the existing SPIN and BAS model. Thus, the proposed model increases the performance of the network. It also increases the network lifetime by saving battery power of the nodes.

Table 1. Power consumption betweenSPIN,BAS and proposed model.

Power consumption	**SPIN (μJ)**	**BAS(μJ)**	**Proposed(μJ)**
P_{Tx}	1,340	130	66.12
P_{Rx}	1,205	210.5	122.5
P_{Kx}	0	0.73	.63
P_{tot}	2545	341.13	125.3

Table 2. Packet Transmission Quotient comparison between the models.

	SPIN	BAS	Proposed model
Total packets overhead $MTotx = MS\ x+MRx$	6	3	2

5.2 Packet transmission quotient

The network efficiency is denoted by the time taken to transmit the data on the network. The packet header stores the format information as an additional byte. The overall speed of transmission of the raw data is reduced due to this additional byte added to the assembling and disassembling of packets. In the SPIN protocol when an adversary node joins the network, the message is forwarded to the base station which will increase the traffic and in turn reduce the efficiency of the network. In the BAS protocol,any node sends ID [2 bytes] to authenticator node which responds with a seed[8 bytes], and afterwards, an encryption key[16 bytes] is sent to authenticator node which is used for node identification. Thus, authenticator transmits only one packet and receives 2 packets. In the proposed model the sender device will send 1 packet and the IP address is verified with the Cluster head which will forward the packet and only the actual receiver can receive the packet and respond back to the sender device. Hence it will receive only one packet. Therefore the packet transmission quotient is reduced for the device. Table 2 compares the packet transmission quotients of SPIN, BAS and the proposed models. Figure 1 compares the performance of the proposed model with those of existing wireless models (SPIN and BAS) and Fig 2 is used to identify the malicious node proving that the prescribed model is better than other models if IP's of Source and Destination does not match.

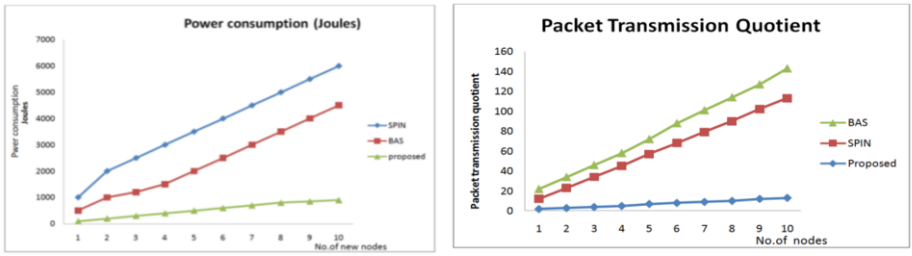

Figure 1. Comparison of Performance of power consumption and Packet Transmission Quotient of the proposed algorithm

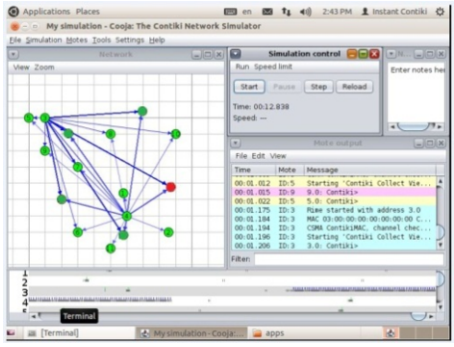

Figure 2. Identification of Malicious node using proposed algorithm

6. Conclusion

The simulation results prove the proposed model outperforms the existing wireless schemes SPIN and BAS. .The future enhancement in the proposed method is to incorporate inside security measures against attacks (e.g DoS attacks) integrity and confidentiality of data.

References

[1] Aluvala, Srinivas, K. Raja Sekhar, and Deepika Vodnala.(2016) .A novel technique for node authentication in mobile ad hoc networks. Perspectives in Science 8: 680-682.

[2] Devi, C. S.and S.A. Arunmozhi (2015). Cluster based Authentication Scheme (CBAS) for Secure Routing in MANET, 121(8), 36–41.

[3] K. Govil,(2014) .Cluster Head Selection Technique For Optimization Of Energy Conservation In MANET. pp. 39–42.

[4] K. H. M. Wong, Y. Zheng, J. Cao, and Wang.A dynamic user authentication scheme for wireless sensor networks. in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp. 318–327, 2006.

[5] K. Kaur,(2015).Weightage based Secure Energy Efficient Clustering Algorithm in MANET. pp. 1006–1012.

[6] Preet, Raman, Paramjeet Singh, and Shaveta Rani.A Node Authentication Mechanism for Securing MANETs.International Journal of Advanced Research in Computer Science 8.4 (2017).

[7] Riaz, Rabia, et al. BAS: the biphase authentication scheme for wireless sensor networks. Security and Communication Networks 2017 (2017).

[8] Rizvi, Sanam Shahla, and Tae-Sun Chung. Investigation of in-network data mining approach for energy efficient data centric wireless sensor networks. International Review on Computers and Software 8.2 (2013): 443-447.

[9] S. Aruna and A. Subramani,(2014).Comparative Study of Weighted Clustering Algorithms for Mobile Ad Hoc Networks. vol. 4, no. 5, pp. 307–311.

[10] Xiao, Debao, Meijuan Wei, and Ying Zhou. Secure-spin: Secure sensor protocol for information via negotiation for wireless sensor networks.(2006) 1ST IEEE Conference on Industrial Electronics and Applications. IEEE, 2006.

[11] V.D.Ambeth Kumar (2017), Efficient Routing for Low Rate Wireless Network a Novel Approach. International Journal of Image Mining, Vol. 2, Nos. 3/4, 2017