Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 579 – 586

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Mathematical Model of Security Framework for Routing Layer Protocol in Wireless Sensor Networks

Ganesh R. Pathak[a], Suhas H. Patil[b]

[a]*Dept. of Computer Science and Engineering, Sathyabama University, Jeppiaar Nagar, Rajiv Gandhi Road, Chennai-600119, Tamil Nadu, India,*
[b]*Dept. of Computer Engineering, Bharati Vidyapeeth University College of Engineering, Pune-411043, Maharashtra, India*

Abstract

Most of the environmental and non-attended applications of Wireless Sensor Networks (WSN's) need mobile sensor nodes. However, mobility of sensor nodes increases security issues in WSNs and it's also vulnerable to various kinds of attacks. Dynamic WSN emerges two most common issues related to the authentication of moving sensor nodes and security in communication and key distribution. After possible movement of sensor node requires authenticating again and again from the base station or some other trusted nodes. Similarly, confidentiality in communication and key distribution is an important factoragainst man-in-middle type of attacks. Till the day most of the WSN's security researchers concentrate on the static environment. Though there schemes are secure and efficient but not sufficient to secure mobile WSN's environment. In this paper we have proposed a novel protocol framework and related mathematical model for secure routing layer communication and key distribution in mobile WSN's. After that we apply this model for performance evaluation on the basis of static as well as dynamic scenario for different number of nodes which shows that our framework is satisfactorily suitable for dynamic WSNs applications.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords:Wireless Sensor Networks; authentication; key distribution; mobility; Message Authentication Code

1. Introduction

WSN's domain has gained more popularity in research field. The reason behind this popularity is not only due to its applications but due to its co-domain fields also such as security, authentication, key management, routing, data aggregation, and disseminations etc.[10].

Basically WSNs consist of heterogeneous[4, 5] type of small devices that is sensor nodes those having small size, less memory[6, 9], limited battery power like properties along with the sensing capabilities. Sensor nodes can sense its

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.121

surrounding environment to collect information related to the events happening in its range and based on some set of rules they disseminate that information to the base station via a wireless medium.

Most of the WSN's researcher's focuses on static sensor nodes which need one time authentication in WSNs. However dealing with mobile sensor nodes can pose different types of challenges and security related issues. Challenges are nothing but mobile node increases data transmission failure rate due to continuous route change in the network as well as increase in packet delivery delay which leads to bad affect in real time applications. Similarly, security related issues[7] like mobile nodes need authentication and re-authentication due to change in region as well as they are very prone to various types of both active and passive attacks by attackers or intruders also.

Whenever a mobile sensor node (slave node) connects to the WSN then sink node (master node) has to authenticate that slave node. In case mobile node moves to the range of another master node, master node needs to authenticate that slave node again. Hence, in high mobility environment master nodes need to authenticate slave nodes again and again though it had authenticated before by any other master nodes in the same network. Similarly, for node to node communication privacy plays an important role because intruders can tamper in between communication and make damage by changing information. Dissemination of authenticated key in WSNs is one of the basic security problems. As sensor nodes are light-weight devices and have limited memory and limited computational power[9], making the use of security protocols of other computer networks to WSNs is not enough. As a result, the primary issues in security researches on WSN are the design of resource-efficient security protocol. A number of approaches such as pre-distribution and hierarchical key management schemes, pair-wise key agreement and group based key agreement were introduced for the efficient authenticated key distribution[1, 2, 8]. So that our main goals are to reduce the load of frequent authentication, increase confidentiality and provide key freshness framework.

This paper is organized into five sections. The previous section covers the Introduction. Next section describes the proposed protocol description. Section 3 explains actual mathematical model of proposed protocol framework for secure routing layer protocol. Section 4 describes performance evaluation and the final section concluded the paper.

2. SRL protocol description

In this section we have described our proposed protocol framework for secure routing layer communication and key distribution in dynamic WSNs. Figure 1 show the block diagram of our proposed protocol which consists of base station (BS), two master nodes (S1, S2) and a slave node (N). This framework is divided into five stages viz.

a. Stage 0: Determination and Discovery of Master Nodes.
b. Stage 1: Master Nodes Communication Set-up.
c. Stage 2: Master Nodes Distribution of Authentication Keys.
d. Stage 3: Primary Authentication of Slave Nodes.
e. Stage 4: Secondary Authentication of Slave Nodes.

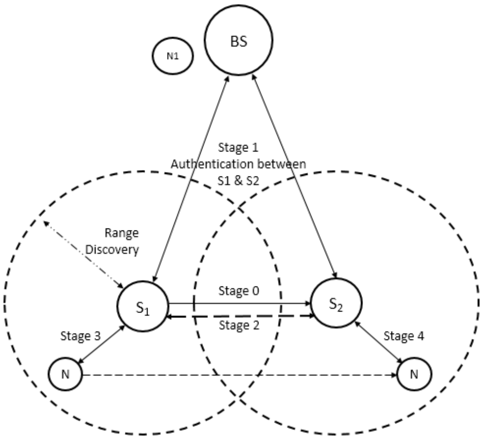

Figure 1: Block diagram of proposed framework

2.1. Stage-0: Determination and discovery of master nodes

In first stage where master nodes start to communicate with its 1 hop neighboring master nodes by broadcasting an authentication packet in WSNs. This authentication packet generally contains a hello message, a random number R and current timestamp, along with these things packet also contains a Message Authentication Hash Code (MAC hash code) to verify its confidentiality at receiver side. MAC hash code identify whether received packet is secure or some man-in-middle attack happened over there. The master node S1 generates an authentication packet which consists of R and its current timestamp T broadcasted in WSNs.

2.2. Stage-1: Master nodes communication set-up

Whenever a master node receives an authentication packet broadcasted by its neighboring master nodes, it initiates the process of communication set-up. Master node generates a new R. Along with newly generated R, master node sends a received authentication packet and MAChash code for verification purpose to the base station. On the other side base station verifies both authentication packets and generates two different response packets by exchanging random numbers received by both the authentication packets through which both the master nodes generate an integrity key by using one way key derivation function and received random numbers.

In stage 0 and stage 1 the master node S2 generates an authentication packet which contains a new R with previous authentication packet of master node S1 and sends it to the base station BS. Base station in figure 3, after getting an authentication packet from master node S2 it generates two response packets RP for S1 and S2 by exchanging their random numbers to develop integrity key using one way key derivation function and received random numbers of S1 and S2.

2.3. Stage-2: Master nodes distribution of authentication keys

This is the stage where master nodes need to share authentication keys to its neighboring master nodes so that, it generates a two different seed values and send it to the respective neighboring master nodes. Master nodes who received those seed values then they generates authentication keys which will help in secondary slave node re-authentication process. The master node S1 and S2 shares their seed values to generate an authentication keys for each other.

2.4. Stage-3: Primary authentication of slave nodes

This is an independent stage for primary authentication of slave nodes. If a slave node is not authenticated at all from any of the master node in WSN then there is need to authenticate slave node from that master node in the range slave node comes first. Whenever a slave node received broadcasted authentication packet of master node from stage 0 it generates a R. Slave node sends a response packet RP to the master node which contains newly generated R, authentication packet of master node and MAC hash code for verification purpose. After getting response packet from slave node a MAC hash code generated by master node for received packet and send it to the base station with response packet. Here, base station verifies the MAC hash codes of master and slave nodes and generates two response packets by exchanging their random numbers through which master node and slave node generates an authentication tickets and related MAC hash code. This is the way how slave node authenticated by a master node.

2.5. Stage-4: Secondary authentication of slave node

When slave node moves continuously in WSN and try to authenticate from other master nodes then stage-3 process is necessary if and only if it is new master node or it is not neighbor of previous authenticated master node. Other than this only needs to re-authenticate slave node from neighbor master node. Whenever slave node N received an authentication packet of new master node it generates and sends a packet to new master node which contains its authentication ticket of previous master node and MAChash code of its authentication ticket. Master node then provide a new authentication ticket to slave node on successful verification and this way slave node re-authenticated by new master node.

3. Proposed mathematical model for secure routing layer protocol

Secure Routing Layer Protocol (SRLP) is our proposed protocol framework for secure routing layer communication and key distribution between master and slave nodes. Consider a WSN environment of 40 numbers of nodes placed in network randomly from which we have selected one node as base station some nodes as master nodes and others are slave nodes.

Here P is the set of phases P= $\{P_1, P_2, P_3, P_4, P_5\}$

1. **Stage-0 : $P_1 = \{AP_I, E_I, M_I\}$**

Where,I = {1, 2, 3….10}

P_1 = Discovery and determination of master nodes.

AP_I = Authentication Packet of master nodes I.

E_I = Encrypted Packet of master node I.

M_I = MAC for master node I.

$AP_I = S_I$+"*HELLO*"$+E_I+M_I$

S_I = Identification of Ith master node.

$E_I = R_I \oplus T_I$

$h:(h(E_I) \oplus h(S_I)) \rightarrow M_I$

$E_I = E_K\ (E_I \oplus S_I)$

Here, E_K = Encryption function.

R_I = Random number of Ith master node.

T_I = Current time stamp.

h = Regular hash function.

S_I: $AP_I \rightarrow$ Network.

2. **Stage 1 : $P_2 = \{P_{2(a)}, P_{2(b)}, P_{2(c)}, P_{2(d)}\}$**

Where,P_2 = Master nodes communication setup.

a) $P_{2(a)} = \{AP_J, E_J, M_J, M_J\}$

Where,J = {1, 2, 3….10}

AP_J = Authentication Packet of master nodes J.

E_J = Encrypted Packet of master node J.

M_J = MAC for master node J.

$AP_J = S_J+B_{ID}+S_I+M_I+E_J+M_J$

S_J = Identification of Jth master node.

B_{ID} = Identification of base station.

$E_J = R_J \oplus E_I$

$h:(h(E_J) \oplus h(S_J) \oplus h(B_{ID}) \oplus h(S_I) \oplus h(M_I)) \rightarrow M_J$

$E_J = E_K\ (E_J \oplus S_J)$

Here, D_K = Decryption function.

R_J = Random number of Jth master node.

S_J: $AP_J \rightarrow B_{ID}$

b) $P_{2(b)} = \{RP_B, E_{BI}, E_{BJ}, M_{BI}, M_{BJ}\}$

RP_B = Response Packet of base station for connection setup.

E_{BI} = Encrypted Packet of base station for Ith master node.

E_{BJ} = Encrypted Packet of base station for Jth master node.

M_{BI} = MAC of base station for Ith master node.

M_{BJ} = MAC of base station for Jth master node.

$RP_B= B_{ID}+S_J+S_I+E_{BJ}+M_{BI}+M_{BJ}$

$D_K\ (E_J \oplus S_J) \rightarrow E_J$

If $M_J = h(h(S_J \oplus B_{ID} \oplus S_I \oplus E_J \oplus M_I))$

$E_I \oplus E_J \rightarrow R_J$

If $M_I = h(h(E_I \oplus S_I))$

$E_I \oplus T_I \rightarrow R_I$

$E_{BI} = R_J \oplus T_I$

$h: (h(B_{ID}) \oplus h(S_J) \oplus h(E_{BI})) \rightarrow M_{BI}$

$E_{BJ} = R_I \oplus E_{B1}$

$h:(h(B_{ID}) \oplus h(S_J) \oplus h(R_J) \oplus h(E_{BJ}) \oplus h(M_{BI})) \rightarrow M_{BJ}$

$E_{BI}=E_K (E_{BI} \oplus B_{ID})$

$E_{BJ}=E_K (E_{BJ} \oplus B_{ID})$

$B_{ID}: RP_B \rightarrow S_J$

c) $P_{2(c)} = \{RP_{JI}, K_{IJ}, IK_{IJ}, M_{JI}\}$

RP_{JI} = Response Packet of J^{th} master node for I^{th} master node.

K_{IJ} = Shared encryption key of I^{th} and J^{th} master node.

IK_{IJ} = Integrity Key of I^{th} and J^{th} master node.

M_{JI} = MAC of J^{th} master node for I^{th} master node.

$RP_{JI} = S_J+S_I+E_{BI}+M_{BI}+M_{JI}$

If $M_{BJ} = h(h(B_{ID}) \oplus h(S_J) \oplus h(E_{BJ}) \oplus h(M_{BI}) \oplus h(R_J))$

$D_K (E_{BJ} \oplus B_{ID}) \rightarrow E_{BJ}$

$K_{IJ} = K_F (0 \oplus R_I \oplus R_J)$

$IK_{IJ} = K_F (1 \oplus R_I \oplus R_J)$

$h:(h(S_J) \oplus h(S_I) \oplus h(R_I) \oplus h(R_J)) \rightarrow M_{JI}$

$S_J: RP_{JI} \rightarrow S_I$

d) $P_{2(d)} = \{ACK_C, K_{IJ}, IK_{IJ}, M_{IJ}\}$

ACK_C = Acknowledgment packet for communication setup.

M_{IJ} = MAC of I^{th} master node for J^{th} master node.

$ACK_C = S_I+S_J+$"ACK"$+M_{IJ}$

If $M_{JI}=h(h(S_J) \oplus h(S_I) \oplus h(R_I) \oplus h(R_J))$

$D_K (E_{BI} \oplus B_{ID}) \rightarrow E_{BI}$

$K_{IJ} = K_F (0 \oplus R_I \oplus R_J)$

$IK_{IJ} = K_F (1 \oplus R_I \oplus R_J)$

$h: (h(S_I) \oplus h(S_J) \oplus h(R_I) \oplus h(R_J)) \rightarrow M_{IJ}$

$S_I: ACK_C \rightarrow S_J$

3. Stage 2 : $P_3 = \{P_{3(a)}, P_{3(b)}\}$

Where,P_3 = Master node's distribution of authentication key.

a) $P_{3(a)} = \{AKP_I , E_{AI}, M_{AI}\}$

AKP_I = Authentication Key Packet of master node I.

E_{AI} = Encrypted authentication key packet of I^{th} master node.

M_{AI} = MAC for an authentication key packet of I^{th} master node.

$AKP_I = S_I+S_J+E_{AI}+M_{AI}$

$E_{AI} = R_{ASEED} \oplus R_{AI}$

$h: (h(S_I) \oplus h(S_J) \oplus h(E_{AI})) \rightarrow M_{AI}$

$E_{AI} = E_K (S_I \oplus E_{AI})$

Here,R_{ASEED} = Random seed value of I^{th} master node.

R_{AI} = Random number of I^{th} master node.

$S_I: AKP_I \rightarrow S_J$

b) $P_{3(b)} = \{RKP_J, AK_I, AIK_I, M_{AJ}\}$

RKP_J = Response Key Packet of J^{th} master node.

AK_I = Authentication Key of I^{th} master node.

AIK_I = Integrity Authentication Key of I^{th} master node.

M_{AJ} = MAC for response key packet of J^{th} master node.

$RKP_J = S_J+S_I+$"ACK"$+M_{AJ}$

If $M_{AI} = h(h(S_I) \oplus h(S_J) \oplus h(E_{AI}))$

$D_K (E_{AI} \oplus S_I) \rightarrow E_{AI}$

$R_{ASEED} = E_{AI} \oplus R_{AI}$

$AK_I = K_F (0 \oplus R_{ASEED})$

$AIK_I = K_F\ (1\oplus R_{ASEED})$

$h{:}\ (h\ (S_I)\oplus h(S_J)\oplus h(AIK_I)) \rightarrow M_{AJ}$

S_J: $RKP_J \rightarrow S_I$

4. **Stage 3 : $P_4 = \{P_{4(a)}, P_{4(b)}, P_{4(c)}, P_{4(d)}, P_{4(e)}\}$**

Where,P_4= Primary authentication of slave node.

a) $P_{4(a)} = \{AP_N, E_N, M_N\}$

$N = \{11, 12\ldots39\}$

AP_N = Authentication packet of N^{th} slave node.

E_N = Encrypted packet of N^{th} slave node.

M_N = MAC of N^{th} slave node.

$AP_N = S_N+S_I+E_N+M_N$

S_N = Identification of N^{th} slave node.

$E_N = R_N\oplus E_I\oplus M_I$

$h{:}\ (h(S_N)\oplus h(S_I)\oplus h(E_N)) \rightarrow M_N$

S_N: $AP_N\rightarrow S_I$

b) $P_{4(b)} = \{AP_{NI}, M_{NI}\}$

AP_{NI} = Primary authentication packet of I^{th} master node for N^{th} slave node.

M_{NI} = MAC of I^{th} master node for N^{th} slave node.

$AP_{NI} = S_I+B_{ID}+S_N+E_N+M_N+M_{NI}$

$h{:}(h(S_I)\oplus h(B_{ID})\oplus h(S_N)\oplus h(E_N)\oplus h(M_N))\rightarrow M_{NI}$

$E_I = E_K\ (E_I\oplus S_I)$

S_I: $AP_{NI}\rightarrow B_{ID}$

c) $P_{4(c)} = \{RP_{NB}, E_{BN}, M_{BN}, E_{BI}, M_{BI}\}$

RP_{NB} = Response of authentication packet of base station.

E_{BN} = Encrypted packet of base station for N^{th} slave node.

M_{BN} = MAC of base station for N^{th} slave node.

E_{BI} = Encrypted packet of base station for I^{th} master node and N^{th} slave node.

M_{BI} = MAC of base station for I^{th} master node and N^{th} slave node.

$RP_{NB} = B_{ID}+S_I+E_{BI}+M_{BI}$

If $M_{NI}=h(h(S_I)\oplus h(B_{ID})\oplus h(S_N)\oplus h(E_N)\oplus h(M_N))$

$D_K(E_I\oplus S_I) \rightarrow E_I$

$R_N = E_N\oplus E_I\oplus M_I$

$E_{BN} = R_N$

$h{:}(h(B_{ID})\oplus h(S_N)\oplus h(S_I)\oplus h(E_{BN})) \rightarrow M_{BN}$

$E_{BI}= S_N\oplus E_{BN}\oplus M_{BN}$

$h{:}(h(S_I)\oplus h(B_{ID})\oplus h(S_N)\oplus h(R_N)\oplus h(E_{BN})) \rightarrow M_{BI}$

$E_{BI} = E_K\ (E_{BI}\oplus B_{ID})$

B_{ID}: $RP_{NB}\rightarrow S_I$

d) $P_{4(d)} = \{RP_{IN}, K_N, AT_{NI}, M_{ANI}, E_{IN}, M_{IN}\}$

RP_{IN} = Response Packet of I^{th} master node for Nth slave node.

K_{NI} = Encryption key for N^{th} slave node from I^{th} master node.

AT_{NI} = Authentication Ticket of N_{th} slave node from I^{th} master node.

M_{ANI} = MAC for authentication ticket of N^{th} slave node from I^{th} master node.

E_{IN} = Encrypted packet of I^{th} master node for N^{th} slave node.

M_{IN} = MAC of I^{th} master node for N^{th} slave node.

$RP_{IN} = S_I+S_N+E_{BN}+M_{BN}+E_{IN}+M_{IN}$

If $M_{BN} = h(h(S_I)\oplus h(B_{ID})\oplus h(S_N)\oplus h(R_N)\ )\oplus h(E_{BN}))$

$D_K(E_{BI}\oplus B_{ID}) \rightarrow E_{BI}$

$E_{BN} = E_{BI}\oplus S_N$

$K_{NI} = K_F\ (R_I\oplus R_N)$

$AT_{NI} = T_I\oplus R_N\oplus K_{NI}$

$h{:}\ (h(S_N)\oplus h(AT_{NI})) \rightarrow M_{ANI}$

$E_{IN} = AT_{NI}\oplus M_{ANI}\oplus T_I$

$h{:}(h(S_I)\oplus h(S_N)\oplus h(R_I)\oplus h(E_{IN}))\rightarrow M_{IN}$

$E_{BN} = E_K\ (E_{BN}\oplus S_I)$

Here,K_F = One way key derivation function.

S_I: $RP_{IN}\rightarrow S_N$

e) $P_{4(e)} = \{ACK_{NI}, M_{AI}\}$

ACK_{NI} = Acknowledgment packet of N^{th} slave node for authentication ticket.

M_{AI} = MAC of N^{th} slave node for I^{th} slave node.

$ACK_{NI} = S_N+S_I+M_{AI}$

If $M_{IN} = h(h(S_I)\oplus h(S_N)\oplus h(R_I)\oplus h(E_{IN}))$

$D_K(E_{BN}\oplus S_I)\rightarrow E_{BN}$

$h{:}\ (h(S_N)\oplus h(S_I)\oplus h(R_N)\oplus h(R_1))\rightarrow M_{AI}$

S_N: $ACK_{NI}\rightarrow S_I$

5. Stage 4: $P_5 = \{P_{5(a)}, P_{5(b)}, P_{5(c)}\}$

Where,P_5 = Secondary authentication of slave node.

a) $P_{5(a)} = \{AP_{NJ}, M_{NJ}\}$

AP_{NJ} = Authentication Packet of N^{th} slave node for re-authentication.

M_{NJ} = MAC of N^{th} slave node for re-authentication.

$AP_{NJ} = S_N+S_J+AT_{NI}+M_{ANI}+M_{NJ}$

$D_K\ (E_J\oplus S_J)\rightarrow E_J$

$h{:}(h(S_N)\oplus h(S_J)\oplus h(AT_{NI})\oplus h(M_{ANI})\oplus h(E_J))\rightarrow M_{NJ}$

S_N: $AP_{NJ}\rightarrow S_J$

b) $P_{5(b)} = \{RP_{JN}, K_{NJ}, AT_{NJ}, M_{ANJ}, E_{JN}, M_{JN}, M_{RJ}\}$

RP_{JN} = Response Packet of J^{th} slave node for re-authentication.

K_{NJ} = Encryption key for N^{th} slave node from J^{th} master node.

AT_{NJ} = Authentication Ticket of N_{th} slave node from J^{th} master node.

M_{ANJ} = MAC for authentication ticket of N^{th} slave node from J^{th} master node.

E_{JN} = Encrypted packet of J^{th} master node for N^{th} slave node.

M_{RJ} = MAC of J^{th} master node for encryption key.

M_{JN} = MAC of J^{th} master node for N^{th} slave node.

$RP_{JN} = S_J+S_N+E_{JN}+M_{JN}$

$K_{NJ} = K_F\ (R_J\oplus R_N)$

$AT_{NJ} = R_N\oplus K_{NJ}$

$h{:}(h(S_N)\oplus h(AT_{NJ}))\rightarrow M_{ANJ}$

$h{:}(h(K_{NJ})\oplus h(R_J))\rightarrow M_{RJ}$

$E_{JN} = R_J\oplus M_{RJ}\oplus AT_{NJ}\oplus M_{ANJ}$

$h{:}(h(S_N)\oplus h(S_J)\oplus h(M_{ANJ}))\rightarrow M_{JN}$

S_{ID2}: $R_{RT}\rightarrow N_{ID1}$

c) $P_{5(c)} = \{ACK_{NJ}, M_{AJ}\}$

ACK_{NI} = Acknowledgment packet of N^{th} slave node for re-authentication ticket.

M_{AI} = MAC of N^{th} slave node for J^{th} slave node.

$ACK_{NJ} = S_N+S_J+M_{AJ}$

If $AT_{NJ} = R_N\oplus K_{NJ}$

$h{:}(h(S_N)\oplus h(S_J)\oplus h(R_N)\oplus h(R_J))\rightarrow M_{AJ}$

S_N: $ACK_{NJ}\rightarrow S_J$

4. Performance evaluation and result analysis

Maintain a key freshness is a prime need of security and to prevent various types of harmful attacks. In our proposed protocol framework, we have used a technique of random nonce generator to maintain key freshness in wireless sensor network. In our scheme at each and every stage we have generated a random numbers. In stage 0, master nodes broadcast a packet which contains a random number which maintains a uniqueness of broadcasted packet. In stage 1, master node generates a packet for verification purpose and later on to generate integrity keys which contains random numbers. In stage 2, when master nodes wants to share authentication keys with its neighboring master nodes contains a seed value nothing but a random number. Similarly, we have used random numbers for primary and secondary authentication of slave nodes as described in stage 3 and 4 of our proposed protocol framework.

Confidentiality of data aggregation and dissemination is another important issue in wireless sensor networks. We have used a MAChash Code (MAC) in each stage of our proposed protocol framework to verifying confidentiality of transmitted packets in wireless sensor network. If an intruder tampers the packet in between nodes communication, MAC hash code will change its values and at receiver side it will not verify at all.

In our proposed protocol framework when slave node is primarily authenticated by a master node, the slave node obtains an authentication ticket. As slave node moves from its location and ask for the re-authentication to neighboring master node, slave node verifies its authentication ticket from new master node. On successful verification master node provides a new authentication ticket to the slave node. Our technique reduces the work load of base station and respective number of routing control packets.

5. Conclusion

In this paper we have proposed a protocol framework for secure routing layer communication and key distribution in mobile WSN and its respective mathematical model. Basically mathematical model gives us a proper flow of system. Proposed framework is focused on routing overhead in comparison with DSR protocol which gives overall flexible result.

References

1. Gaurish M. Edake, Ganesh R. Pathak and Suhas H. Patil. Secure Localization and Location Verification in Wireless Sensor Networks.*In Proceeding of IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies,* DOI: 10.1109/CSNT.2014.141, pp. 673-676.
2. Kyusuk Han, Kwangjo Kim and Taeshik Shon.Untraceable Mobile Node Authentication in WSN.*in Sensors* 2010 10, 4410-4429; doi:10.3390/S100504410 in April, 2010.
3. Pathak, G.R.; Patil, S.H.; Rana, A.D.; Suralkar, Y.N. Mathematical model for routing protocol performance in NS2: Comparing DSR, AODV and DSDV as example.*in Wireless Computing and Networking (GCWCN), 2014 IEEE Global Conference on* , vol., no., pp.184-188, 22-24 Dec. 2014doi: 10.1109/GCWCN.2014.7030875.
4. Alagheband, M.R.; Aref, M.R. Dynamic and secure key management model for hierarchical heterogeneous sensor networks.*in Information Security, IET* , vol.6, no.4, pp.271-280, Dec. 2012, doi: 10.1049/iet-ifs.2012.0144
5. Rantos, K.; Papanikolaou, A.; Fysarakis, K.; Manifavas, C. Secure policy-based management solutions in heterogeneous embedded systems networks. *in Telecommunications and Multimedia (TEMU), 2012 International Conference on* , vol., no., pp.227-232, July 30 2012-Aug. 1 2012, doi: 10.1109/TEMU.2012.6294723.
6. Subramanian, G.; Amutha, R.Efficient and secure routing protocol for wireless sensor networks using mine detection An extension of triple umpiring system for WSN. *in Computing Technology and Information Management (ICCM), 2012 8th International Conference on* , vol.1, no., pp.141-145, 24-26 April 2012.
7. Murat Dener. Security Analysis in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 303501, 9 pages, 2014. doi:10.1155/2014/303501.
8. Pathak, Ganesh R., Gaurish M. Edake, and Suhas H. Patil. Untraceability of Sensor Node Authentication in Wireless Sensor Networks. *Computational Intelligence and Communication Networks (CICN)*, 2014 International Conference on. IEEE, 2014.
9. Hui-Feng Huang.A New Design of Efficient Key Pre-distribution Scheme for Secure Wireless Sensor Networks. *in Intelligent Information Hiding and Multimedia Signal Processing*, 2007. IIHMSP 2007. Third International Conference on , vol.1, no., pp.253-256, 26-28 Nov. 2007doi: 10.1109/IIH-MSP.2007.41.
10. Chin-Ling Chen; Yu-Ting Tsai; Tzay-Farn Shih. A Novel Key Management of Two-Tier Dissemination for Wireless Sensor Network. *in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2012 Sixth International Conference on , vol., no., pp.576-579, 4-6 July 2012, doi: 10.1109/IMIS.2012.55.