Indian Journal of Science and Technology, Vol 9(10), DOI: 10.17485/ijst/2016/v9i10/88908, March 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Hybrid Novel Perspective of Secure Routing in Wireless Sensor Networks

Ganesh R. Pathak[1]* and Suhas H. Patil[2]

[1]Department of Computer Science and Engineering, Sathyabama University, Jeppiaar Nagar, Rajiv Gandhi Road, Chennai - 600119, Tamil Nadu, India; pathak.gr@gmail.com
[2]Department of Computer Engineering, Bharati Vidyapeeth University College of Engineering, Pune - 411043, Maharashtra, India; suhas_patil@yahoo.com

Abstract

Background/Objectives: Mobile sensor nodes are the key prerequisite for many ecological and non-attended applications of Wireless Sensor Networks. The key objective of this work is to extend the security of roaming nodes to attain the secure routing in WSN.**Methods/Statistical analysis**:Mobility of sensor nodes upsurges security disputes in WSNs and correspondingly it issusceptible to several types ofattacks. We have incorporated the prominentkey distribution tactics like key pre-distribution, hierarchical key management schemes, pair-wise key agreement and group key based key agreement in proposed secure framework. **Findings:**Active wireless sensor network have two utmost issues namely the authentication of mobile nodes and security in communication by means of key distribution. Till the time, many WSN's security practitioners and researchers deliberated about security in WSN in the static environment. Although the schemes available in the literature are secure and effective, they are not adequate for secure roaming WSN's scenario. In this article, we have recommended a hybrid novel perspective of secure routing in WSN. The proposed scheme has been exceedingly effective under dynamic environment and accomplishes significant improvement than existing system in terms of packet delivery ratio, and normalized routing overhead by achieving efficient energy usage.**Applications/Improvements:**We use this novel standard for evaluating the performance of existing traditional secure routing tactics and the proposed secure routing mechanism in static as well as dynamic scenario for several number of wireless sensor nodes. The results deliberated in the last section of this article depicts that the proposed framework for secure routing in WSN is adequatelyappropriate and precise for dynamic WSN applications.

Keywords: Authentication, Key Distribution, Message Authentication Code, Secure Routing,Wireless Sensor Network

1. Introduction

Wireless Sensor Networks (WSN's) domain has gained more popularity in research field due to its ability to support large number of applications. The co-domain fields such as security, authentication, key management, routing, data aggregation and disseminations etc. have all railed attention of researchers in recent years.

WSN considered in this paper consist of heterogeneous[1,2] type of small sensor devices having limited memory[3] and limited battery power along with the sensing capabilities. Sensor nodes can sense its 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 static WSN's research related to security focuses on one time authentication of sensor nodes. 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 end-to-end

*Author for correspondence

delay which leads to bad affect in real time applications. Similarly, security related issues described by Dener[4]like mobile nodes need authentication and re-authentication due to change in region as well as they are prone to various types of active and passive attacks by intruders.

Whenever a mobile sensor node[5,6] (slave node) becomes active then sink node (master node) has to authenticate such node. In case mobile node moves to the range of another master node, master node needs to authenticate the new slave node. Hence, in high mobility environment master nodes need to authenticate slave nodes again and again though it has been 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. Distribution of authenticated key in WSN's is one of the basic security problems. As sensor nodes are light-weight devices and have limited resources, making the use of traditional network security protocols to WSN's is generally not suitable. As a result, the primary issues in security research on WSN are the design of resource-efficient security protocol. A number of approaches such as key pre-distribution, hierarchical key management schemes, pair-wise key agreement and group key based key agreement were introduced for the efficient authenticated key distribution[7–9]. Thus, in this paper we propose a framework to reduce the load of frequent authentication, increase confidentiality and provide key freshness framework.

This paper is organized into five sections. Section 2 describes the proposed secure routing perspective description. Section 3 explains authentic hybrid perspective of secure routing in WSN. Section 4 describes performance evaluation and result analysis and the final section concluded the paper.

2. SRL Perspective Description

In this section we have described the proposed context of Secure Routing for secure communication and key distribution in dynamic wireless sensor networks. Figure 1 show the block diagram of our proposed secure routing perspective which comprises of base station (BS), two master nodes (S1, S2) and a slave node (N). This framework is divided into five phases viz.

a. Phase 1: Determination and discovery of master nodes.
b. Phase 2: Master nodes communication set-up.
c. Phase 3: Master nodes distribution of authentication keys.
d. Phase 4: Primary authentication of slave nodes.
e. Phase 5: Secondary authentication of slave nodes.

2.1 Determination and Discovery of Master Nodes

This is the first phase where master nodes start to communicate with its 1 hop neighboring master nodes by broadcasting an authentication packet in WSN. This authentication packet generally contains a hello message, a random number and current timestamp and message authentication hash code to verify its confidentiality at receiver side. Message authentication code identifies whether received packet is secure or some man-in-middle attack happened before the packet is received at the destination.

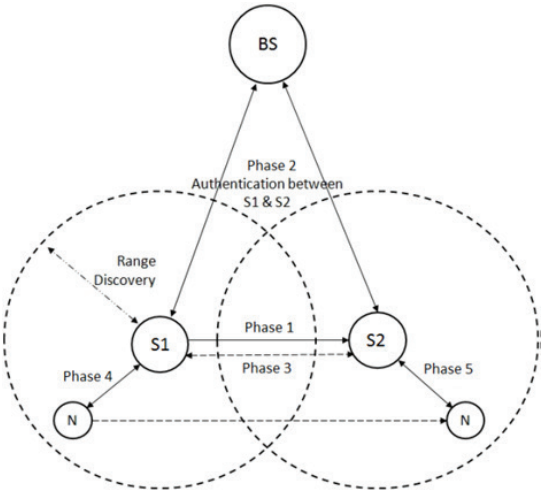

Figure 1. Block diagram of the Expert System

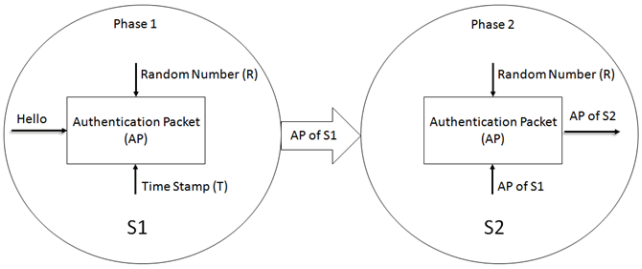

Figure 2. Phase 1 and Phase 2- Determination and discovery of master nodes and primary communication set-up.

As shown in Figure 2, let master node S1 generates and broadcast an authentication packet which consists of a random number R and its current timestamp T.

2.2 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 random number. Along with newly generated random number master node sends a received authentication packet and message authentication hash 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.

As shown in Figure 2, master node S2 generates an authentication packet which contains a new random number 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 Master Nodes Distribution of Authentication Keys

In this phase 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 that receives the seed values, generates authentication keys which will help in secondary slave node re-authentication process.

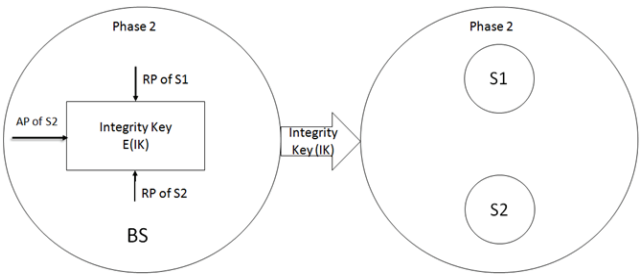

Figure 3. Phase 2- Master nodes communication set-up.

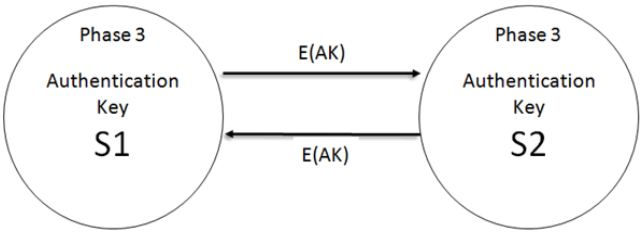

Figure 4. Phase 3 - Master nodes distribution of authentication keys.

As shown in Figure 4, master node S1 and S2 shares their seed values to generate an authentication keys for each other.

2.4 Primary Authentication of Slave Nodes

This is an independent phase for primary authentication of slave nodes. If a slave node is not authenticated by any of the master node, then the master node, in whose communication range the slave node resides, is responsible to perform authentication. Whenever a slave node receives broadcast authentication packet of master node from phase 1 it generates a random number R. Slave node sends a Response Packet (RP) to the master node which contains newly generated random number, authentication packet of master node and message authentication hash code for verification purpose. After getting RP from slave node a message authentication hash code generated by master node for received packet and sends it to the base station with response packet. Here, base station verifies the message authentication hash codes of master and slave nodes and generates two response packet by exchanging their random numbers through which master node and slave node generates an authentication tickets and related message authentication hash code. This is the way how slave node authenticated by a master node.

As shown in Figure 5, slave node N wants to authenticate from master node S1 after getting authentication packet from S1 and hence it generates a random number R. Base station BS exchange random number of N and S1 through which both can generates Authentication Ticket (AT) by using one way key derivation function.

2.5 Secondary Authentication of Slave Node

When a mobile slave node in WSN tries to authenticate itself from a new master node then it follows phase-4

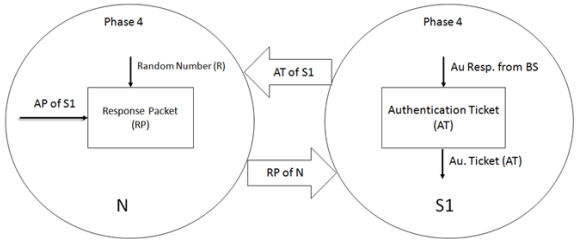

Figure 5. Phase 4 – Primary authentication of slave nodes.

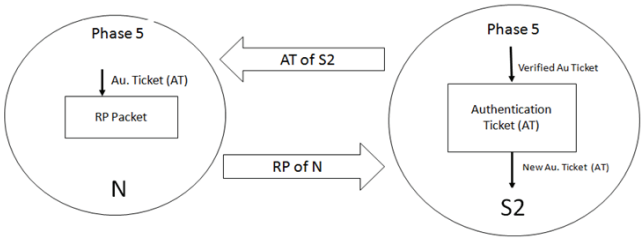

Figure 6. Phase 5 – Secondary authentication of slave node.

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 message authentication hash 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.

As shown in Figure 6, slave node N wants to re-authenticate from master node S2 after its movement so that it generates and sends a response packet to S2 which contains its authentication ticket. Master node S2 gives a new authentication ticket to slave node N on successful verification of previous authentication ticket.

3. Proposed Hybrid Novel Perspective of Secure Routing in WSN

In this section, we have described a novel context of secur-erouting on the basis of Secure Routing Layer Perspective (SRLP) which we have earlier explained in section 2 for secure communication and key distribution between master and slave nodes.

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

1. Phase 1(P_1) = Discovery and determination of master nodes.
   $P_1 = \{AP_I, E_I, M_I\}$
   where,I = {1, 2, 3….10}
   AP_I = Authentication Packet of master nodes I.
   E_I = Encrypted Packet of master node I.
   M_I = Message Authentication Code for master node I.
   $AP_I = S_I + \text{“}HELLO\text{”} + E_I + M_I$
   S_I = Identification of I^{th} 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 I^{th} master node.
   T_I = Current time stamp.
   h = Regular hash function.
   S_I broadcast AP_I in WSN
2. Phase 2(P_2) = Master nodes communication setup.
   P2 = {P2(a), P2(b), P2(c), P2(d)}
   where,
   a) Phase 2(a) ($P_{2(a)}$) = Master node S_J generates authentication packet for base station
   $P_{2(a)} = \{AP_J, E_J, M_J, M_J\}$
   where,J = {1, 2, 3….10}
   AP_J = Authentication Packet of master nodes J.
   E_J = Encrypted Packet of master node J.
   M_J = Message Authentication Code for master node J.
   $AP_J = S_J + B_{ID} + S_I + M_I + E_J + M_J$
   S_J = Identification of J^{th} 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 J^{th} master node.
   S_J sends AP_J to B_{ID}
   b) Phase 2(b) (P2(b)) = Base station exchange of random numbers
   $P_{2(b)} = \{RP_B, E_{BI}, E_{BJ}, M_{BI}, M_{BJ}\}$
   where,RP_B = Response Packet of base station for connection setup.
   E_{BI} = Encrypted Packet of base station for I^{th} master node.
   E_{BJ} = Encrypted Packet of base station for J^{th} master node.
   M_{BI} = Message Authentication Code of base station for I^{th} master node.

M_{BJ} = Message Authentication Code of base station for J^{th} 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 $M_J = h(h(S_J \oplus B_{ID} \oplus S_I \oplus E_J \oplus M_J))$

$E_I \oplus E_J \rightarrow R_J$

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} sends RP_B to S_J

c) Phase 2(c) (P2(c)) = Master node S_J generation of integrity key

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

where,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} = Message Authentication Code of J^{th} master node for I^{th} master node.

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

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

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

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

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

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

S_J sends RP_{JI} to S_I

d) Phase 2(d) (P2(d)) = Master node S_I generation of integrity key

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

where,ACK_C = Acknowledgment packet for communication setup.

M_{IJ} = Message Authentication Code 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 sends ACK_C to S_J

3. Phase 3(P_3) = Master node's distribution of authentication key.

$P_3 = \{P_{3(a)}, P_{3(b)}\}$

where,

a) Phase 3(a) (P3(a)) = Master nodes shares ASEED value

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

where,AKP_I = Authentication Key Packet of master node I.

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

M_{AI} = Message Authentication Code 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 broadcast AKP_I to S_J

b) Phase 3(b) (P3(b)) = Master nodes generates authentication key

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

where,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} = Message Authentication Code 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 sends $RKP_J$to S_I

4. Phase 4(P_4) = Primary authentication of slave node.

$P_4 = \{P_{4(a)}, P_{4(b)}, P_{4(c)}, P_{4(d)}, P_{4(e)}\}$

where,

a) Phase 4(a) (P4(a)) = Slave node authentication packet generation

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

where,N = Number of slave nodes.

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

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

M_N = Message Authentication Code 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 sends AP_N to S_I

b) Phase 4(b) (P4(b)) = Master node MAC generation for slave node

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

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

M_{NI} = Message Authentication Code 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 sends AP_{NI} to B_{ID}

c) Phase 4(c) (P4(c)) = Base station authentication of slave node

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

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

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

M_{BN} = Message Authentication Code 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} = Message Authentication Code 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} sends RP_{NB} to S_I

d) Phase 4(d) (P4(d)) = Master node authentication ticket generation for slave node

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

where,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} = Message Authentication Code 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} = Message Authentication Code 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 sends RP_{IN} to S_N

e) Phase 4(e) (P4(e)) = Slave node authentication acknowledgment

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

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

M_{AI} = Message Authentication Code of N^{th} slave node for I^{th} slave node.

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

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

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

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

S_N sends ACK_{NI} to S_I

5. Phase 5(P_5) = Secondary authentication of slave node.

$P_5 = \{P_{5(a)}, P_{5(b)}, P_{5(c)}\}$

where,

a) Phase 5(a) (P5(a)) = Slave node share authentication ticket to new master node

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

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

M_{NJ} = Message Authentication Code 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 sends AP_{NJ} to S_J

b) Phase 5(b) (P5(b)) = New master node re-authentication of slave node

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

where,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} = Message Authentication Code 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} = Message Authentication Code of J^{th} master node for encryption key.

M_{JN} = Message Authentication Code 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} sends R_{RT} to N_{ID1}

c) Phase 5(b) (P5(b)) = Slave node re-authentication acknowledgment

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

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

M_{AI} = Message Authentication Code 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 sends ACK_{NJ} to S_J

Table 1. Simulation Parameters

Component	Type
Channel Type	Channel/Wireless Channel
Antenna Model	Omni Antenna
Radio Propagation Model	Two Ray Ground
Network Interface Type	Phy/ Wireless Phy
Mac Layer Protocol	IEEE 802.11
Interface Queue Type	Queue/Drop Tail/Pri Queue
Number of Nodes	30, 40, 50, 60, 70
Mobility of Nodes (m/s)	0, 5, 10
Pause Time	30
Topology Size	500m x 500m
Traffic Type	SENSE/UMNAW
Packet Size	512 Byte
Simulation Time	100 seconds
Simulation Tool	NS-2.32

4. Performance Evaluation and Result Analysis

4.1 Simulation Tool and Parameters

The simulation is performed in well-known Network Simulator 2 (NS2) tool[10]. We have set the WSN in 500m X 500m area with number of nodes varying from 30, 40, 50, 60 and 70. In each event driven simulation we have selected 0^{th} node as a base station, 1-9 numbers of nodes as master nodes and remaining as slave nodes. In the network scenario, base station and all of the master nodes are in static mode and slave nodes are in dynamic mode. Other simulation parameters are shown in Table 1.

4.1.1 Result of Performance EvaluationPacket Delivery Ratio

Packet Delivery Ratio calculated using a formula[10].Graph shown in Figure 7(a) is of number of nodes v/s packet delivery ratio of our proposedperspective in various scenarios. "X-axis" shows number of nodes varies from 30, 40, 50, 60 and 70 where "Y-axis shows respective Packet Delivery Ratio (PDR). The graph shows packet delivery ratio when all nodes kept static in nature gives less PDR when numbers of nodes are less. As we increase the nodes PDR also increases. Similarly, when slave nodes kept in mobile environment for maximum velocity of 5 m/s or 10 m/s by keeping hostile environment application in mind such as in military monitoring to tracking tanks and troops. It gives less PDR for less numbers of nodes. As we increase numbers of nodes PDR also increases. Overall dynamic environment gives better result for PDR as compared to static environment.

4.1.2 Normalized Routing Overhead

Normalized Routing Overhead calculated using a formula[10], Total Routing Control Packets/Total Data Packets Send.

Graph shown in figure 7(b) is of number of nodes v/s normalized routing overhead of our proposed framework in various scenarios. "X-axis" shows number of nodes varies from 30, 40, 50, 60, and 70 where "Y-axis" shows respective normalized routing overhead. The graph shows normalized routing overhead increases as number of nodes increases in all scenarios i.e. either in static or in dynamic (maximum velocity of 5 m/s or 10 m/s). The reason behind increasing routing overhead is that we have using broadcast channel in phase 1 where the entire master nodes broadcast its own authentication packets in network time to time as well as if number of slave nodes increases the events/phases also creates more control packets. But still normalized routing overhead provides a better performance in secondary authentication phase as compared to the frameworks whoever needs multiple times authentication to authenticate slave nodes transit from their locations to other locations.

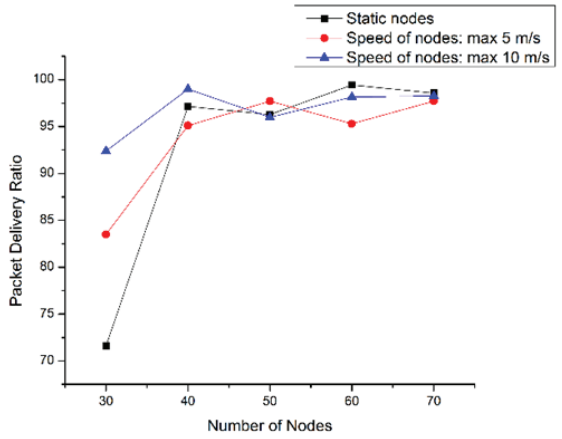

Figure 7(a). Packet Delivery Ratio for 30,40,50,60 and 70 numbers of nodes in static and dynamic scenario.

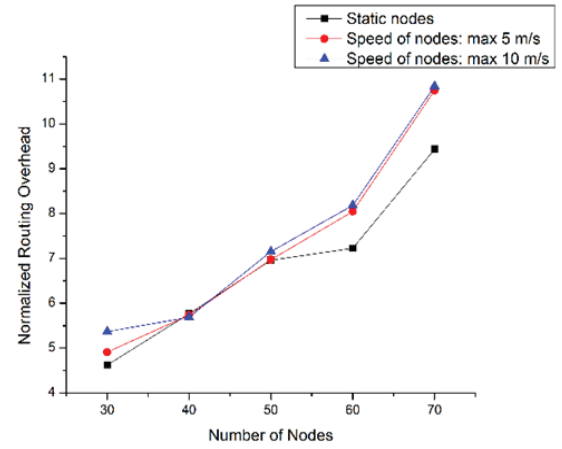

Figure 7(b). Routing Control Overhead for 30,40,50,60 and 70 numbers of nodes in static and dynamic scenario

5. Conclusion

In this paper, we have proposed anovel perspective for secure routing in mobile wireless sensor network in order to attain secure communication and key distribution.A proposed secure routing context enfolds a feasible trust based solution that examines trustworthiness of neighbouring nodes. The simulation results validatethe effectiveness of the mechanism which implies that; the proposed system has been highly effective under dynamic environment circumstances and accomplishes significant improvement than existing system in terms of Packet Delivery Ratio, and Normalized Routing Overhead by achieving efficient energy usage. A proposed routing perspective is time efficient as well as packet traffic efficient since it simplifiesthe substantial improvement in data delivery for dynamic topology with less delay in comparison to the existing traditional routing strategy.

6. References

1. Alagheband MR, Aref M. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. IET Information Security.2012;6(4):271–80.
2. Rantos K, Papanikolaou A, Fysarakis K, Manifavas C. Secure policy-based management solutions in heterogeneous embedded systems networks. 2012 International Conference on Telecommunications and Multimedia (TEMU);Chania;2012.p.227–32.
3. Subramanian G,Amutha R. Efficient and secure routing protocol for wireless sensor networks using mine detection. An extension of triple umpiring system for WSN. 2012 8th International Conference on Computing Technology and Information Management (ICCM);Seoul;2012.p.141–45.
4. Dener M. Security analysis in wireless sensor networks. International Journal of Distributed Sensor Networks. 2014;2014.
5. Krishnakumar SS, Abler RT. Intelligent actor mobility in wireless sensor and actor networks. Proceedings of IFIP International Federation for Information Processing, Wireless Sensor and Actor Networks. Orozco-Barbosa L, Olivares T, Casado R, Bermudez A, editors; Springer: Boston, MA, USA; 2007. p. 13–22.
6. Das S,Liu H, Kamath A,Nayak A,Stojmenovic I. Localized movement control for fault tolerance of mobile robot networks. Wireless Sensor and Actor Networks, Orozco-Barbosa L, Olivares T, Casado R, Bermudez A, editors; Springer: Boston, MA, USA; 2007.p. 1–12.
7. Edake GM, PathakGR,Patil SH. Secure localization and location verification in wireless sensor networks. Proceeding of IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies;Bhopal; 2014.p. 673–76.
8. Han K, Kim K, Shon T. Untraceable mobile node authentication in WSN. Sensors. 2010; 10(5):4410–29.
9. SangeethaK, RavikumarK. A novel traffic dividing and scheduling mechanism for enhancing security and performance in the tor network.Indian Journal of Science and Technology.2015 Apr; 8(7):689–94.doi: 10.17485/ijst/2015/v8i7/62882.
10. Pathak GR, Patil SH, Rana AD, Suralkar YN. Mathematical model for routing protocol performance in NS2: Comparing DSR, AODV and DSDV as example. 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN);Lonavala; 2014.p.184–88.