Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

KEY PRE-DISTRIBUTION SCHEME FOR RANDOMIZED SECURED ROUTING IN WIRELESS SENSOR NETWORKS

U.SENTHIL KUMARAN[1] & ILANGO PARAMASIVAM[2]
[1]Assistant Professor, School of Information Technology, VIT University, Vellore – 632014, India.
[2]Professor, School of Computing Science & Engineering, VIT University, Vellore – 632014, India.
E-mail: [1]senthilkumaran0882@gmail.com

ABSTRACT

In wireless sensor networks (WSN's), majority of its applications necessitate the confidentiality of information they transmit. This can be achieved through secure key management schemes. In this paper, a key pre-distribution scheme for randomized secured routing is proposed for WSN. Initially, the sink utilizes the one hop neighbor information of nodes to predistribute keys. It randomly chooses (n/2) nodes and distributes with (k+m) keys and other nodes obtain (k) keys. Nodes with more shared keys are considered as high resilient nodes. During data transmission, high resilient nodes are preferred to other normal nodes and the next hop is randomly selected from the secured minimum hop neighbors. When there is more than one secure minimum hop links, then a weight function is assigned and the best path is elected. The proposed scheme is simulated in NS-2 and it is shown that it provides high resilience and delivery ratio with reduced energy consumption.

Keywords: *Wireless Sensor Network (WSN), Key Management, Security, Pre-distribution.*

1. INTRODUCTION

1.1 Wireless Sensor Networks

The prominent technology of wireless sensor network (WSN), which is operated to monitor physical environment has been evolved as a result of integrating wireless communications with embedded computing technologies. [1] As of now a wide acceptance is achieved by WSN's. More applications are using tiny wireless sensors to accomplish monitoring, sensing and communication tasks. Most of these applications are adopted in hostile environment, where the success is dependent on its security from malicious attackers. [2]

1.2 Security in Wireless Sensor Networks

WSN comprises of stringent resources namely low battery power, less memory, and associated low energy. Therefore, the sensor nodes are vulnerable to more security attacks. Wireless links are used as a communication channel for sensor nodes. In many cases, sensor nodes are distributed and positioned in hostile environment. Conditions around the environment and resource constraints pave a wide way for security threats in sensor networks. [3] [4] Limited resources, unreliable communications and unattended operations are the three factors to be taken into account before developing a security mechanism in sensor networks. [5]

1.3 Security Requirements in Wireless Sensor Networks

The fundamental requirements to secure WSN are listed below [5]:

- **Data Confidentiality**: In WSN, the term confidentiality refers to the condition that nodes should not disclose the sensed information to their neighbors.
- **Data Integrity**: Data that is forwarded in the network should reach the intended destination without any alteration or changes. This requirement is referred as data integrity.
- **Data Freshness**: Data freshness guarantees that the forwarding messages are new and it assures stale information are not been replayed.
- **Availability**: This security requirement makes sure that informations and security schemes are readily available to the sensor nodes when they required.

1.4 Key Management in WSN

Key management is an important feature of security in wireless sensor networks. The processes such as authentication and privacy are also relied on key management. [6] As like security, key

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

management is also pondered as a cross layer issue. Because, the process of key management is initiated in the link layer and upper layers like network and application layers are also required to forward keys securely. Several security critical applications highly necessitate key management process along with high level of fault tolerance. However, handling both the requirements at the same hand is a daunting task in wireless sensor network as it possesses stringent constraints such as bandwidth and network life time. [7]

1.5 Issues of Key Management

Ensuring confidentiality of information is the main objective of a key management scheme. The defined keys are useful for authenticating legitimate nodes. However, while transmitting data between nodes, an adversary may attempt to crash secret key and can take out confidential information. When we use keys for authentication process, confidential information can be obtained by an adversary by pretending as a legitimate node. At the same time as attempting to crash a key, the attacker stab to understand the message fashions and predicts the secret key. So as to avoid the attackers from predicting keys, a key management scheme has to introduce a rekeying technique at periodic time intervals. Here, the time interval may relies on regularity of communication and key usage.

Apart from above-mentioned issues, adversaries can also make several challenges to a sensor network such as jamming the wireless signals of sensor network, attempting to cause noises and other means to disrupt communications. Further, attacks like jamming can not be managed by key management techniques. [6]

1.6 Problem Identification

Wenjun Gu et al. [8] have proposed a key predistribution scheme. Their scheme has distributed more keys to some nodes so that the links between those nodes tend to have much higher resilience than the link resilience under uniform key pre-distribution. These high resilient links are preferred during routing to enhance the end to end secure communications. But if those high resilient nodes are captured, all these keys can be disclosed. Moreover this work uses GPSR as the routing protocol which uses geographical positions of the nodes. This leads to a high risk of malfunctioning the actual co-ordinates of the nodes.

In order to solve the above problems, in this paper a key pre-distribution scheme for randomized secured routing in WSN is proposed. The paper is organized as related work in section-2, proposed solution in section-3, simulation results in section-4 and conclusion in section-5.

2. RELATED WORKS

Wenjun Gu et al. [8] have designed an end to end secure communication protocol in randomly deployed WSNs. Their protocol is rooted on a methodology known as differentiated key pre-distribution. Their main objective is to share various numbers of key to different sensors to improve the resilience of certain links and then accomplish routing. During data communication, packets in nodes are routed through the links with higher resilience.

Christian Lederer et al. [9] have proposed an energy-efficient implementation of Elliptic Curve Diffie-Hellman (ECDH) Key Exchange for Wireless Sensor Networks. Initially, they have introduced an improved version of hybrid method for multi-precision multiplication. This hybrid method necessitates a fewer single-precision additions. To lessen the execution time of ECDH key exchange at the expense of a slight increase in memory requirements, they have utilized fast algorithms for elliptic curve scalar multiplication (window method, comb method). Finally, they have considered schemes for securing their ECDH implementation against side-channel attacks.

Arif Selcuk Uluagac et al. [10] have proposed an energy-efficient Virtual Energy-Based Encryption and Keying (VEBEK) scheme for WSNs. The authors have initiated their work with an objective of lessening the number of transmissions requiring for rekeying to avoid unused and old keys. Their VEBEK's secure communication framework has presented a technique to verify data in line. After the verification, their technique drops false packets from malicious nodes. By this process, their VEBEK's manages the lifetime of the sensor network. Further, their technique has updated the keys without exchanging control messages for key renewals.

Shu Yun Lim et al. [11] have proposed two group key management schemes. They have presented those schemes with the aim of conserving energy by keeping the cryptographic burden on sensors with higher computation power, the access points and on forwarding nodes. Both of the key management schemes enable a sensor network to set up cryptographic keys in an autonomous fashion. Their first technique requires a small amount of keys independent of the network size,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and hence achieves high scalability. A group key establishment scheme is introduced as a second technique with initial shared keys for authenticating and establishing a set of secure group-wise local links.

A key re-distribution and authentication based technique for secured communication in clustered wireless sensor networks with node mobility is proposed in [12] by Saswati Mukherjee et al. To establish secure communication in network the authors have considered a hierarchical cluster based WSN. They have exploited Improved key distribution mechanism (IKDM) to employ key distribution. Whenever nodes move from one cluster head (CH) to another key re-distribution is evolved. Further, they have constructed an authentication model to recognize an intruder in a cluster.

Haijun Liang and Chao Wang [13] have presented a new energy efficient dynamic key management for wireless sensor networks. Initially they divide a cluster into many virtual grid and there is only one node is active in a grid to reduce energy consumption. Then they have adopted a scheme to achieve dynamic key management, namely, pair-wise key based on common polynomial and random number.

Pengcheng Zhao et al. [14] have proposed a hybrid key management scheme. Their scheme is based on clustered wireless sensor networks. They have built a d-dimensional key tree between cluster head and base station using shared function to generate front-end session key. Cluster members generate their own key and adjacent key pair based on the information of their geographic location and pre-loaded master key.

3. PROPOSED SOLUTION

3.1 Overview

In this paper, a random key pre-distribution scheme for secured routing in wireless sensor network (WSN) is proposed. Initially after the nodes are distributed in the network, the sink divides the nodes into multiple classes and utilizes the one hop neighbor information of nodes to distribute keys. The sink randomly selects (n/2) nodes of a node's neighbors and allocates with (k+m) keys whereas other remaining nodes are acquire (k) keys. As soon as predistribution of keys is finished, each node constructs all possible direct and indirect key paths to their neighbors. With help of constructed paths the pair wise key is established between neighbors. For data transmission the proposed scheme makes use of Non-Repetitive Random Propagation (NRRP) routing algorithm. When a node desires to transmit data to the sink, the next hop is randomly selected from the secured minimum hop neighbors. In the event such as when there is the presence of more than a secure minimum hop links, then weight function is assigned and the best path is elected.

3.2 Network Architecture

Consider the wireless sensor network with N_i number of sensor nodes, where i= 1, 2 … n with a sink node S. These N_i nodes are randomly distributed in the network. It is assumed that the sink (S) is preinstalled with a set of K keys in the key pool. The S is the in charge of randomly distributing keys to all nodes in the network. The schematic diagram of the network is shown in figure-1.

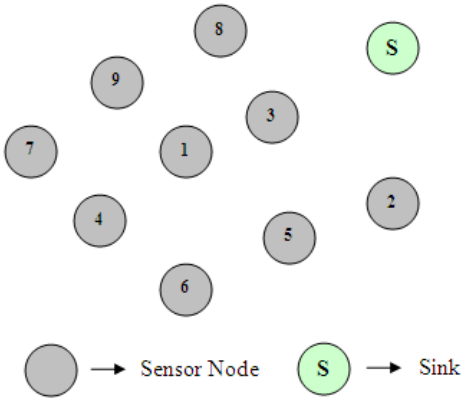

Figure-1 Wireless Sensor Network

Once the nodes are distributed in the network, every node explores its one hop neighbors by sending HELLO messages. Nodes that receive HELLO messages respond back to the sender. By collecting replies, node N_i constructs neighbor table (NT) and the format of NT is given below in table-1,

Table-1 Format of HELLO message

Node ID	Sequence Number	Neighbor Node ID	Key ID

In the above table, Key ID will be discussed in later section. Once NT tables are constructed by nodes, it sends the collected neighborhood information to the sink.

3.3 Distinguished Key Pre-Distribution Scheme

The distinguished key predistribution scheme supposes that nodes are secured and they can not be

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compromised before predistribution of keys. The proposed distinguished key predistribution scheme consist of two phases namely initial key pre-distribution and pair wise key generation.

3.3.1 Initial Key Pre-distribution

Initially, the sink (S) partitions the nodes into H number of classes such that N_i $(1 \le i \le H)$ nodes. The technique describes the nodes according to their class names. For instance, nodes in i^{th} class are defined as class i nodes and so on. Then, the sink selects distinct keys K_i $(1 \le i \le H$ and $K_1 \ge K_2 \ge ... \ge K_H)$ from the key pool of size K and shares out to nodes in class i.

In order to distribute secret keys to nodes in a group, the sink makes use of NT information of a node. As it is described in section-3.2, each node constructs NT by collecting one-hop neighborhood information. Consider node N_i of i^{th} class has *n* one-hop neighbors, and then the sink randomly selects (n/2) one-hop neighbors and shares (K_i+m) keys, where m is a changeable variable. Other nodes in the NT table will obtain K_i keys. The nodes are selected by the sink randomly and it does not depend on any parameters.

Since, (n/2) nodes are selected randomly to distribute K_i+m keys; it is difficult for an adversary to disclose all keys by compromising a single node. This process is repeated by the sink until nodes in entire groups are distributed with predistributed secret keys. Nodes that possess K_i+m keys have high resilience against failures. Further, these nodes assure an extra reliability and security when compare with nodes with K_i keys. Therefore, while transmitting data between any pair of source and destination, nodes with K_i+m keys are preferred to other nodes.

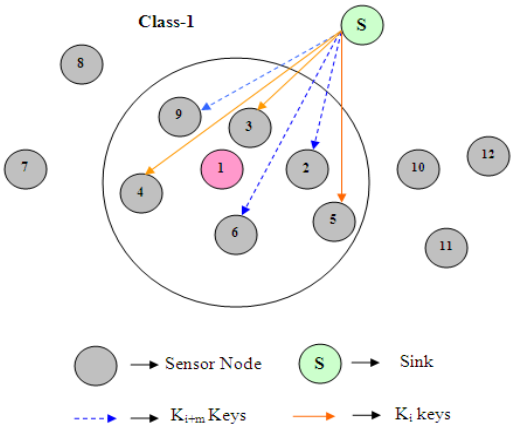

Figure-2 Key Distribution Phase

Consider the sketch given in figure-2, the sink (S) invokes the key predistribution phase as nodes are distributed in the network. Figure-2 includes the nodes that correspond to class-1. To distribute keys, initially the S exploits NT of node N_1. The node N_1 has six neighboring nodes namely N_2, N_3, N_4, N_5, N_6 and N_9. Among six neighbors (n=6), the S randomly chooses (6/2) (i.e) three nodes namely N_2, N_6 and N_9 and distributed with K_{i+m} keys. Other nodes namely N_3, N_4 and N_5 obtain K_i keys.

Algorithm-1 describes the process of initial key pre-distribution

Algorithm-1

1. Let H be the set of classes i, where i=1, 2 … H and S be the Sink
2. Consider N as a set of sensor nodes and n as the number of neighboring nodes
3. Let NT_i be the neighbor table of node N_i
4. Consider K_i and K_{i+m} as keys taken from the key pool of size K
5. Nodes are distributed and S is positioned in the network
6. S classifies the nodes into H classes
7. It selects the class i from H and chooses node N_i from N
8. S acquires NT_i and calculates n
9. It calculates (n/2)
10. Randomly selects (n/2) nodes and distributes K_i+m keys to them
11. S distributes K_i keys to the remaining nodes in NT_i
12. Steps 5 to 11 are repeated until S reaches the class H

3.3.2 Pair Wise Key Generation

As soon as the sink completes the predistribution of keys to nodes, every sensor node forwards K-info message to their one-hop neighbor. K-info message contains the key-ID's information. Subsequently, every node receives a set of K-info messages from its one-hop neighbors. The key ID information of neighboring nodes is keep tracked in Key ID of NT. By utilizing this information, every node generates direct and indirect key paths with its neighbors. Here, direct key path refers to one-hop key path and indirect key path denotes two-hop key path. The construction of direct and indirect key paths is as follows.

(i) When node N_i distributes keys with node N_{i+1}, then node N_i generates a direct key path with N_{i+1}. The node N_i can construct as many as "Direct key paths" to their neighbors.

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(ii) When node N_i desires to generate indirect key path with node N_{i+2}, then it first forwards a request message to all its neighbors including the node id's of N_i and N_{i+2}. Once, the neighboring node (say N_{i+1}) receives the request, it checks whether it has shared predistributed keys with both node N_i and N_{i+2}. If so node N_{i+1} forward back a reply to node N_i. Thus, N_i generates Indirect key path as,

$N_i \longrightarrow N_{i+1} \longrightarrow N_{i+2}$

A node can construct many "Indirect key paths" regardless of "Direct key path" along any specific node.

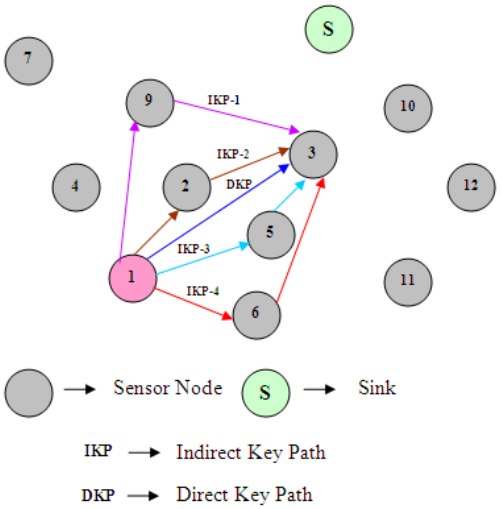

Figure-3 Direct and Indirect Key Paths Construction

Take into account the picturization given in figure-3. In that, node N_1 creates direct and indirect key paths to node N_3. It constructs only one direct key path described as DKP and four indirect key paths namely IKP-1, IKP-2, IKP-3 and IKP-4.

After a node (N_i) constructed all possible "Direct and Indirect key paths" to an another node (N_{i+1}), node N_i will produce multiple random shares and forwards every key share on every key path such as Direct and Indirect key paths. With the use of combination of XOR, all key shares are encrypted/decrypted hop by hop along the path. Eventually, the combination of all the key shares that is forwarded between node N_i and N_{i+1} is termed as the pair wise key of those two nodes. This generated pair wise key is used for securing transmission during routing.

3.4 Route Selection

To route data from any node to the sink, in this paper we enhance the Non-Repetitive Random Propagation (NRRP) routing algorithm. [15]

3.4.1 Weight Function Computation

In order to calculate the weight function of a path, let us consider the distinguished key predistribution scheme given in section 3.3. Assume K(i,j) as the number of keys shared between node N_i and N_j. This information can be obtained from the trusted offline authority (OA). Then the number of defense keys (D(i,j)) between N_i and N_j can be given as,

$$D(i,j) = K(i,j) + \sum_{g=1}^{T} \min(K(i,OA_g), K(OA_g,j)) \quad (1)$$

In the above expression, T denotes the number of indirect key paths between N_i and N_j. The defense keys define strength of a link. Through this, we can describe how resilient the link is.

To perform data communication, node N_i assigns weight to all its neighboring nodes. The weight function is as follows,

$$W_{Nj} = \frac{D(i,j)^{\beta}}{\sum_{k \in M(i)} D(i,k)^{\beta}} \quad (2)$$

Here, node N_i assigns weight only to the nodes to which it has established pair wise keys. Let M(i) be the set of secure neighboring nodes of node N_i, which are closer to the sink than itself. W_{Nj} is the weight probability that node N_i selects N_j as the forwarder. β is referred as priority variable. The value of β can be assigned as per the requirement of communication as,

If (β =0) then
Equal priority will be given to all nodes in M(i)
Else if (β =positive value) then
Higher priority will be given to more resilient links
Else if (β = infinity) then
Most resilient links are selected for routing
End if

3.4.2 Non-Repetitive Random Propagation (NRRP) Routing Algorithm

When node N_i intends to transmit data to the sink, it utilizes the M(i) nodes for transmission. M (i) is the set of secure neighboring nodes of N_i, where it has established pair wise secret key with them. First, it randomly selects a node from M(i) and transmits a data packet. Similarly, data packets are transmitted. To enhance the efficiency of propagation and to assure loop-free routing, NRRP routing algorithm includes the node-in-route (NIR) field. Initially, this field is set to zero. Whenever a data packet is forwarded from a node to another

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

node, the corresponding node ID is appended in NIR field such that the source does not select the same node again and again. Thus, when determining next hop, the node N_i selects a minimum and secure next hop from M(i). In case, when the source has more minimum hop secure paths, then weight function (W_{Nj}) is utilized. The node N_i assigns weight function to each path and chooses the best path.

Merits of Proposed Scheme

- In the distinguished key predistribution scheme, as (n/2) nodes are selected randomly to distribute K_i+m keys; it is difficult for an adversary to disclose all keys by compromising a single node.
- The enhanced Non-Repetitive Random Propagation (NRRP) routing algorithm increases efficiency in propagation and assures loop free routing paths.

4. SIMULATION RESULTS

4.1 Simulation Parameters

The key pool size K is a critical parameter because in random key distribution schemes the amount of storage reserved for keys in each node is likely to be a preset constraint, which makes the size of the key ring R a fixed parameter. Once R is set, then for larger values of K the probability that two nodes will share a key is small. Node initialization at the network bootstrapping phase is also simulated.

The proposed Randomized Secure Routing (RSR) is evaluated through NS-2 [16] simulation. We consider a random network of sensor nodes deployed in an area of 500 X 500m. The number of nodes is varied as 50,100,150 and 200. The sink node is assumed to be situated 100 meters away from the above specified area. The simulated traffic is CBR with UDP. The number of clusters formed is 9. Out of which, data is transmitted from 4 cluster heads to the sink. Three sensor nodes in each cluster are sending data to their cluster head. The transmission rate is varied from 100 to 300kb.

The node capturing attack is simulated. The percentage of attacker nodes is fixed as 5% of the total number of nodes in the network.

Table- 2 Simulation Parameters

No. of Nodes	100
Area Size	500 X 500
Mac	802.11
Routing protocol	RSR
Simulation Time	25 sec
Traffic Source	CBR
Packet Size	512 bytes
Attackers	10 to 30
Transmission Range	250m
Transmit Power	0.395 w
Receiving power	0.660 w
Idle power	0.035 w
Initial Energy	10 Joules

4.1 Performance Metrics

The performance of RSR is compared with the Differentiated Key Management scheme of [8]. The performance is evaluated mainly, according to the following metrics.

- **Energy**: It is the average energy consumed for the data transmission.
- **Delay**: It is the average time taken by the packets to reach the destination.
- **Fraction of Compromised communications:** It denotes how a node capture affects the rest of network resilience. It is calculated by estimating the fraction of communications compromised between non compromised nodes by captured nodes
- **Average Packet Delivery Ratio:** It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Based on Attackers

In order to see the effect of node capturing attack when the number of compromised nodes is varied, the number of compromised nodes is varied as 10,15,20,25 and 30 in the 100 node scenario.

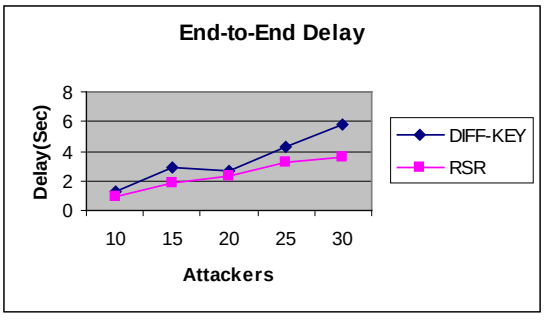

Figure 4: Attackers Vs Delay

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

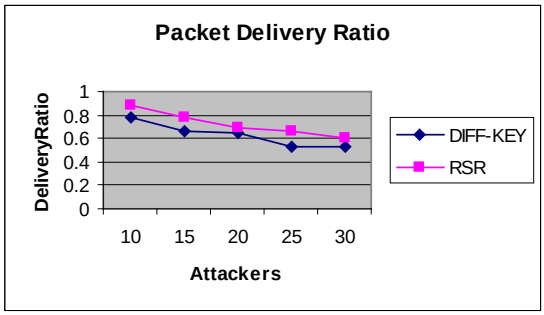

Figure 5: Attackers Vs Delivery Ratio

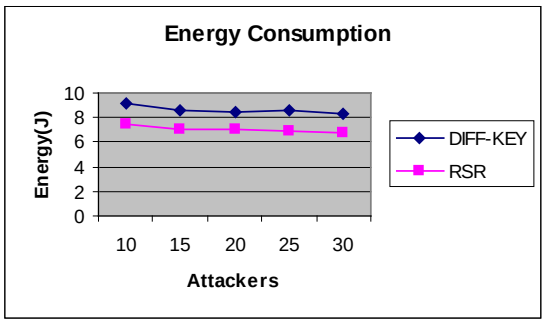

Figure 6: Attackers Vs Energy

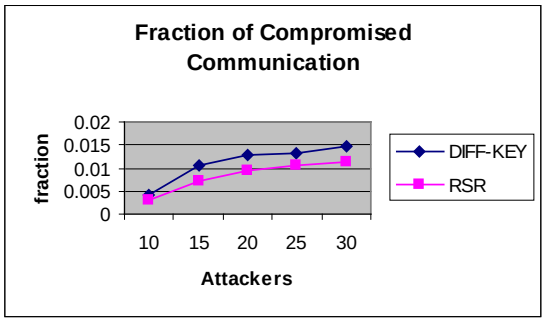

Figure 7: Attackers Vs Compromised communications

Figure 4 shows the delay occurred for both the techniques when the number of compromised nodes is increased. It is trivial that the delay increases, with the increase in compromised nodes. Bur the delay of RSR is 28% less than DIFF-KEY technique, because of the hierarchical routing protocol we applied

Figure 5 shows that the packet delivery ratio decreases when the number of compromised nodes is increased. From the figure we can see that the delivery ratio of RSR is 13.2% higher than DIFF-KEY technique.

The average energy consumption values for both the techniques are given in Figure 6. Since higher residual energy nodes are selected as cluster heads, RSR attains 18.2% less energy consumption than DIFF-KEY technique.

The resillience against node capture result is given in Figure 7. For the increased number of compromised nodes, RSR shows 24% better performance for resilience. This because of the cluster based key pre-distribution scheme of DIFF-KEY.

5. CONCLUSION

In this paper, a key pre-distribution scheme for randomized secured routing in WSN is proposed. Initially, using a distinguished key pre-distribution scheme, the sink utilizes the one hop neighbor information of nodes to predistribute keys. It randomly chooses (n/2) nodes and distributes with (k+m) keys and other nodes obtains k keys. Nodes with more secure keys are considered as high resilient nodes. For data transmission the proposed scheme makes use of Non-Repetitive Random Propagation (NRRP) routing algorithm. When a node desires to transmit data to the sink, the next hop is randomly selected from the secured minimum hop neighbors. Since, (n/2) nodes are selected randomly to distribute (k+m) keys; it is difficult for an adversary to disclose all keys by compromising a single node. Simulated results show that it provides high resilience and delivery ratio with reduced energy consumption.

REFERENCES

[1] Sasha Slijepcevic, Vlasios Tsiatsis, Scott Zimbeck," On Communication Security in Wireless Ad-Hoc Sensor Networks", *Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02)* 1080-1383/02 $17.00 © 2002 IEEE

[2] WenjunGu, XiaoleBai, Sriram Chellappan and Dong Xuan, "Network Decoupling for Secure Communications in Wireless Sensor Networks", 2006

[3] Saurabh Singh, Dr. Harsh Kumar Verma, "Security For Wireless Sensor Network", Vol. 3 No. 6 June 2011

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb. 20-22, 2006 ICACT2006

[5] Rajeshwar Sing, Singh D.K. and Lalan Kumar, "A review on security issues in wireless sensor network", *Journal of Information Systems and Communication*, ISSN: 0976-8742 & E-ISSN: 0976-8750, Vol. 1, Issue 1, 2010, PP-01-07

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] Syed Muhammad Khaliq -ur-Rahman Raazi, Zeeshan Pervez and Sungyoung Lee, "Key Management Schemes of Wireless Sensor Networks: A Survey ", 2009

[7] Johnson C. L Ee and Victor C. M. Leung, U Niversity Ofbritishcolumbia, "Key Management Issues in Wireless Sensor Networks: Current Proposals And future developments", *IEEE Wireless Communications* • October 2007 1536-1284/07/$20.00 © 2007 IEEE

[8]. Wenjun Gu, Neelanjana Dutta, Sriram Chellappan, and Xiaole Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks", *IEEE Transactions on Network and Service Management*, Vol. 8, No. 3, September 2011.

[9] Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großsch¨adl ,Alexander Szekely, and Stefan Tillich, "Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks", *WISTP 2009, LNCS 5746*, pp. 112–127, 2009. IFIP International Federation for Information Processing 2009

[10]. Arif Selcuk Uluagac, Raheem A. Beyah, Yingshu Li, and John A. Copeland, "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks", *IEEE Transactions on Mobile Computing*, VOL. 9, NO. 7, JULY 2010.

[11]. Shu Yun Lim and Meng-Hui Lim, "Energy-Efficient and Scalable Group Key Management for Hierarchical Sensor Network", *Journal of Ubiquitous Systems & Pervasive Networks*, Volume 2, No. 1, 2011.

[12] Saswati Mukherjee,Matangini Chattopadhya, Samiran Chattopadhyay, Amrita, "A Key Re-Distribution and Authentication Based Technique For Secured Communication In Clustered Wireless Sensor Networks with Node Mobility", *International Journal of Computer Networks & Communications* (IJCNC) Vol.2, No.6, November 2010

[13].Haijun Liang and Chao Wang, "An Energy Efficient Dynamic Key Management Scheme Based on Polynomial and Cluster in Wireless Sensor Networks", *Journal of Convergence Information Technology*, Volume 6, Number 5. May 2011.

[14]. Pengcheng Zhao, Yong Xu and Min Nan, "A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks", *Wireless Sensor Network*, doi:10.4236/wsn.2012.48029 Published Online August 2012.

[15] Tao Shu, Marwan Krunz, and Sisi Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes", *IEEE Transactions on Mobile Computing*, pp- 941-954, 2010