DRFSD: DIRECTED RESTRICTED FLOODING FOR SECURE DATA-AGGREGATION IN WIRELESS SENSOR NETWORKS

[1]LATA B T, [2]RAGHAVENDRA M, [3]SUMUKHA T V, [4]SUHAS H, [5]TEJASWI V, [6]SHAILA K, [7]VENUGOPAL K R, [8]L M PATNAIK

[1,2,3,4,6,7]Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore
[5]Department of CSE, National Institute of Technology, Surathkal, India
[8]Honorary Professor, Indian Institute of Science, Bangalore, India.
E-mail: Lata_bt@yahoo.co.in

Abstract- Secured Data Transmission is a major issue in Wireless Sensor Networks (WSNs). In this paper we have proposed Directed Restricted Flooding Protocol (DRFSD) in WSNs. This protocol is better than H-SPREAD (Hybrid Security Protocol for REliable dAta Delivery). In DRFSD, alternate multipaths are selected based on the sensor node, that are placed at 180◦ direction with the Base Station (BS). This scheme is efficient in sending the Data Packets to the Base Station in shorter duration than the H-SPREAD. Simulation Results show that our algorithm approach performs well with respect to latency in comparison with earlier algorithms.

Keywords- Restricted Flooding, DATA-Aggregation, GPS, Multipath Routing.

I. INTRODUCTION

Wireless sensor networks are characterized by small, battery-powered, limited resources, less memory and with broadcast communication capabilities. Current Wireless Sensor Network routing protocols are still struggling to find valid paths between source and destination. Security is a major challenging issue in Wireless Sensor Networks. In this paper we address secure routing issues in the wireless sensor networks. Multipath routing can be used for maximum utilization of network resources.

Mulipath routing is capable of aggregating the resources of multiple paths and reducing the blocking capabilities, allowing the data transfer at high rate when compared to a single path. Multipath routing does effective load balancing and also provides security. If we split the packets of the same message, and transfer them on multiple paths, then the malicious node present on a path, can hack only a portion of the data.
Flooding is one of the important techniques used to transfer the data on multiple paths. By transferring the data packets on multiple paths, it avoids the adversary to get the complete data.

A. Motivation:
Wireless Sensor Networks are prone to security breaches.

Security is important during data aggregation or data transmission. Most of the existing algorithms provides security by consuming more time and takes long paths for data transmission. For delay sensitive applications, time is vital and hence we have to develop a scheme that provides security utilizing minimum latency.

B. Contribution:
We have developed DRFSD which provides security and consumes less data transmission time than the existing al-gorithms by selecting the multiple paths based directional routing with the BS. DRFSD protocol helps in overcoming the disadvantages present in H-SPREAD. DRFSD is direction based, where multiple paths are selected based on the nodes, which are placed at 180◦ degree direction with the BS. Since, it is direction based, zigzag motion is reduced when compared with the H-SPREAD. We split data packets of a single message and transfer it on different multiple paths. Even if the attacker captures the node, entire data cannot be hacked.

C. Organization:
The rest of the paper is organized as follows: Section 2 discusses briefly about the related work. Section 3 states Background study and section 4 the problem definition. Section 5 describes the architecture of the network model. Algorithms are discussed in Section 6. Section 7 gives the description of the implementation and the performance analysis of the algorithms. Conclusions are presented in Section 8.

II. LITERATURE SURVEY

Wenjing et al., proposed Security Protocol for Reliable dAta Delivery (SPREAD), in which secret messages are split into shares (different parts of a message) by secret sharing schemes and then these shares are delivered to different multiple node disjoint paths to the destination. Even if a few nodes are compromised, the message as a whole is not hacked. It is possible that selected multiple paths may take longer distances.

Wenjing et al., introduced hybrid multipath scheme (H-SPREAD) to improve security and reliability of the WSNs. It is based on a N-to-1 multipath discovery protocol, which is able to find multiple node-disjoint paths from recovery sensor node to the base station simultaneously in one route discovery process. It enhances the security of end-to-end data delivery with secret sharing. It uses active per-hop packet salvaging strategy to improve the reliability. In this strategy, before the frame is removed from the buffer, each node knows whether the transmission is successful or not. The H-SPREAD protocol is based on simple flooding.

Swades et al., presented a Meshed Multipath Routing (M-MPR) protocol with Selective Forwarding (SF) of packets and end-to-end Forward Error Correction (FEC) coding. The meshed multipath searching scheme is suitable for sensor networks that has reduced signaling overhead and nodal database. M-MPR achieves a much improved throughput over conventional disjoint multipath routing with comparable power consumption and receiver complexity; FEC and Selective Forwarding (SF) consumes much less network resources, such as channel bandwidth, battery power and packet replication.

Chris et al., proposed threat models and security goals for routing in sensor networks. Sinkhole attacks and HELLO floods have been introduced to provide secure routing. Reza et al., introduce a BSMR (Byzantine-Resilient Secure Multicast Routing) is a secure on-demand multicast protocol for multi hop wireless networks. It provides resiliency against Byzantine attacks (Black hole, Wormhole and flood rushing). It uses selective data forwarding mitigation mechanism based on a reliability metric that captures adversarial behavior.

Min-Ho et al., proposed a new group key management scheme for multiple multicast groups, called the Master-Key-Encryption-based Multiple Group Key Management (MKE-MGKM) scheme. It exploits asymmetric keys, i.e., a master key and multiple slave keys, which are generated from the proposed master key encryption (MKE) algorithm, is used for efficient distribution of the group key. It alleviates the re-keying overhead by using the symmetry of the master and slave keys. Even if one of of the slave keys is updated, the remaining ones can still be unchanged by modifying only the master key. It reduces the storage and the communication overhead.

Anfeng et al., [8] formulated the secret-sharing-based multipath routing problem as an optimization problem. Three-phase disjoint routing scheme called the Security and Energy-efficient Disjoint Route (SEDR) is proposed. It consists of regional dispersive routing, disjoint identical-hop routing and least-hop routing. It delivers sliced shares to the sink node with randomized disjoint multipath routes by utilizing the available surplus energy of sensor nodes, such that network security is maximized without decreasing the lifetime of WSNs.

Karunakaran et al., proposed a key management scheme, which establishes shared keys with their communicating neighbor. It generates randomized multipath routes for secure transmission of data to the sink. In heterogeneous sensor networks, Elliptic Curve cryptography has been used for efficient key management, which is more efficient, scalable, highly secure and reduces communication overhead. The routes generated by this scheme are highly dispersive, energy efficient and are quite capable of bypassing the black holes, at low energy cost.

Salman et al., presented the design of a landmine detection system capable of detecting landmines, Improvised Explosive Device (IEDs) and Unexploded Ordances (UXOs). This system has the capability to identify multiple scanner operating units and relays the landmines detected by them on to the base station via Zigbee modules. The algorithm can detect mines and plot their respective positions on the map. The system offers flexibility and support for integration with Unmanned Ground Vehicle (UGV) and robotic manipulator for future innovations. Multiple UGV's instead of multiple operating units and an intelligent system can be designed to plan the path of these vehicles accordingly.

Gupta et al., surveyed on the secure routing protocols in wireless sensor networks. Saranya et al., proposed a Secure On Demand Multicast Routing Protocol (S-ODMRP). It is a secure high-throughput multicast protocol that incorporates a novel defense scheme Rate Guard. Rate Guard combines measurement-based detection and accusation-based reaction techniques, which addresses the metric manipulation and packet dropping attacks. It eliminates outsider attacks, message spoofing, modification attacks.

Shancang et al., have developed an adaptive load-balancing multipath routing protocol (SM-AODV) for Wireless Sensor Networks, that uses load balancing, congestion control and secure delivery scheme to address the limitations in existing multipath routing schemes. In SM-AODV, the packets are delivered across multipaths using a secure and reliable scheme. It achieves substantial improvement in routing downstream traffic by using a secret sharing scheme at the source. It also adopts an adaptive congestion control scheme, which is effective even in the case of frequent node and link failures. Encrypting the data and sending on multiple paths can provide better security.

Hannes analyzed the cost function properties and General lower bound expressions for multicast trees.

The author has considered multicast trees with optimally placed intermediate forwarding nodes and derived an upper bound for the cost of such tree. The procedure is illustrated by three cost functions, namely, the euclidean distance, the energy consumption. the expected number of retransmissions underRayleigh fading.

Sankardas introduced synopsis diffusion approach which secures the data aggregation at Base Station in Wireless sensor Networks, in the presence of attack. Simulation results show that the per-node communication overhead does not increase with the network size.

Chen designed a dynamic trust management protocol for secure routing optimization in Delay tolerant networks (DTNs) in the presence of well-behaved, selfish and malicious nodes. It maximizes the delivery ratio than the Bayesian and PROPHET (Probabilistic Routing in Intermittently Connected Networks) protocol by incurring the message overhead. This work can be extended to other trust based applications.

III. BACKGROUND STUDY

Wenjing et al., introduced hybrid multipath scheme (H-SPREAD) to improve security and reliability of the WSNS. It involves the typical task of disseminating data requests from a base station to all sensor nodes and to collect readings from every sensor node back to the base station. It involves end-to-end multipath data dispersion, combined with secret sharing. It also uses, N-to-1 multipath discovery protocol which initiates a route update periodically or on demand at the base station. At the end of each discovery process, every sensor node has a set of node-disjoint paths back to the base station.

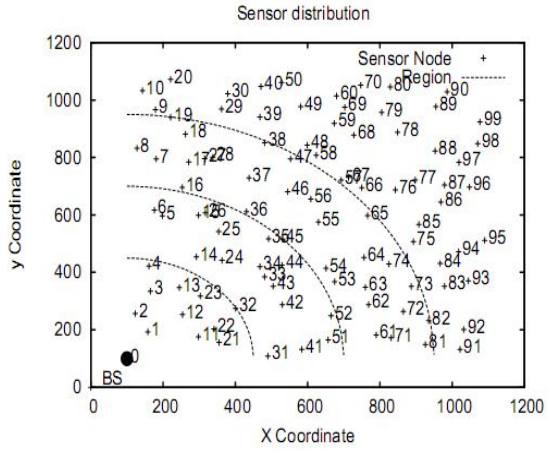

Fig. 1. Sensor nodes distribution in DRFSD into four ranges.

IV. MODEL AND PROBLEM DEFINITION

A. Problem Definition

The major constraints in WSNs are limited resources. The computation and the communication power of a sensor node is restricted with a limited battery life and small amount of memory. We must achieve quicker data delivery and provide

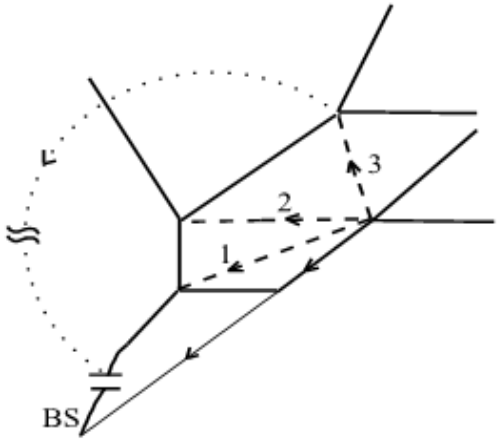

Fig. 2. H-SPREAD (Utilizes all possible paths to the destination. Here, paths used are three(which are marked as 1, 2, 3)).

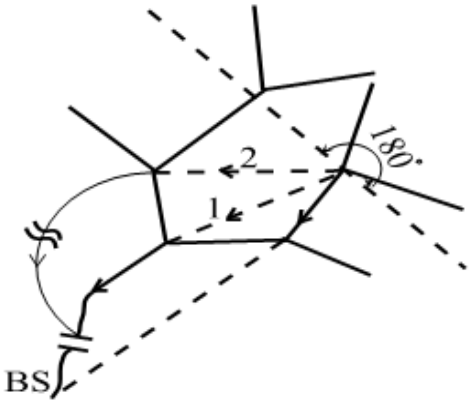

Fig. 3. DRFSD (Utilizes the possible paths in the direction of 180◦ from Base Station (BS). Here paths selected are two(which are marked as 1 and 2).)

as much security that the application demands. The objectives of this work are to

1) Minimize the latency.

2) Reduce the number of hop counts and increase the secure delivery probability.

V. NETWORK MODEL

The network model is a randomly deployed sensor nodes with the base station placed at left bottom corner. The area of node deployment is considered to be 1000m x 1000m with the base station positioned close to the origin at (100, 100), as shown in Fig. 1. The remaining nodes are deployed randomly. The base station is placed at the bottom left corner of the deployment area, so that it is outside the danger zone. Hence, in case any accidents occur in the deployment site and the base station is not affected. Sensor is activated on the occurrence of an event. Encryption algorithms are applied to the shares (split data packets) and they are transmitted to multiple nodes. The nodes, which satisfy the direction and angle criteria are

selected for multiple paths. This establishes secure route between sensor node and the Base Station.

A. Assumptions

1) All the nodes are GPS (Geographical Positioning System) enabled.
2) Nodes are aware of their neighboring node IDs, xy co-ordinates, angle and distance.
3) GPS system decides first and last nodes.

VI. ALGORITHMS

In H-SPREAD, there is a zigzag motion. Multiple paths in this algorithm may include longer distances. Since, the number of paths are more and may include longer distances, it gives a chance for more number of malicious nodes (Figure 2). We propose DRFSD that gives better results than H-SPREAD in terms of path length and security.

A. DRFSD

DRFSD is a highly directionality centric approach to reduce the chances of transmitting packets in longer paths and in meaningless directions. In this algorithm, 100 GPS (Global Positioning System) enabled, self configured, sensors are randomly deployed. The path selection process is based on whether the next node is in the direction of the destination or not. To do so, we consider a 180◦ sector oriented towards the base station. Once flooding is initiated, alternate path selection is done based on the 180◦ direction. Only neighboring nodes which are situated towards base station are selected for alternate paths as shown in Figure 3. (The steps are given in Algorithm 1.)

By considering a 180◦ sector, we present the selection of nodes that are always away from the Base Station. Repeating the path selection procedure at every hop until the base station ensures high directionality of the path (Figure 3). There will always be forward movement only. The chances of zigzag propagation as seen in H-SPREAD is also reduced to a very great extent. (Difference is observed in the Figures 2, 3.)

Algorithm 1: Directed Restricted Flooding Protocol for Secure Data-aggregation (DRFSD).

variable :start(First node in the surrounding list),
$last$(Last node decided by the GPS system),
$dist1$(distance between BS and SN(sensor node)),
$dist2$(Distance of BS and node i),
NN_i (neighboring node i)
Input: Range(300 mtrs)
Output: EfficientDataDelivery_on_Shorter_Distance.

for ($i = start$ to $last$) **do**
if ($dist1 > dist2$) **then**
  $data$=encrypt(packet);
  $send(data, NN\_i)$;
end for;
return EfficientDataDelivery_on_Shorter_Distance;

Alternate paths (which are exceeding one) are marked in the figures, 2, 3, respectively, In Figure 2, Paths traversed will be longer. In Figure 3, smaller number of paths and less distances are traversed.

VII. IMPLEMENTATION AND PERFORMANCEEVALUATION

A. Implementation

The security of the network can be disturbed by the adversary. The adversary can deploy the nodes, can block, or hijack the data, or send wrong information to the BS or may filter the data so that the latest information is not available to the BS. To address these issues, we have introduced DRFSD that reduces unnecessary traffic and saves energy. We have restricted multiple paths in order to make the data secure. Even if the packet is blocked by the malicious node, the data travels in the alternate path, so that data delivery is guaranteed. Nodes are deployed randomly in the first quadrant as shown in Fig.1. Network consists of N number of nodes. The angles of all the nodes with respect to Base station is calculated by GPS. To keep the setup economical, we use GPS enabled nodes at critical positions. GPS nodes are deployed such that, they cover maximum distance. Non GPS nodes calculate their position relatively to the GPS station. Since, there exists multiple paths in the network, it is difficult for the adversary to guess all the alternate paths and deploy the nodes.

TABLE I
SIMULATION PARAMETERS

Simulator	NS3
Duration	20 Sec
Sample Rate	1 sec
Area	1000m*1000m
Radio Range	300m
Thres Dis	175m
Thres temp	75 Deg. C
Thres pres	675 mmHg
Thres smoke	40 mg/L

TABLE II
PARAMETERS OF EVALUATION

Latency
Residual Energy
Delivery Probability
Malicious node packet delivery

B. Simulation Setup

Simulation is done using NS3. Deployment consists of 1000m*1000m. 100 nodes are deployed. Transmission range is set to 300 meters. Simulation is run for maximum of 15 secs. Simulation results are obtained for related residual energy, path length, number of packets delivered, delivery probability and number of malicious nodes in the network.

C. Performance Evaluation

Samples are taken for every 1 sec. Table I describes the parameters used for simulation. Latency, Residual Energy, Delivery Probability, Malicious node packet

delivery are the parameters to be evaluated. (see table II). The paper compares DRFSD[1] Vs HSPREAD[2].
The sensor nodes are arranged in 1000*1000 square

[1]Directed Restricted Flooding for Secure Data-aggregation Protocol for Secure Data Collection in Wireless Sensor Networks (DRFSD)

[2]A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks (H-SPREAD)

meter area, as shown in Fig. 1. The total deployment region is divided into four, for analyzing purposes. This is shown for analyzing the node behavior in various regions, in terms of energy consumption. The nodes near the base station i.e., in the 1st region or in the borders near the base station are found to be critical nodes. They consume more energy compared to nodes which are situated far away from the base station. The four regions are divided based on distance/radius from the base station The base station is located at (0,0) in the deployment region. The points in the graphs are shifted vertically and horizontally by 100 points in order to have clarity.

The position of the base station is located in the bottom left corner or south-west. It is located outside the deployment area i.e., outside the critical region, where accidents such as fire, enemy intrusion etc., does not occur. It is possible to connect the base station with IPV6 gateway so that data cannot be accessed via Internet. The base station can be easily replaced, corrected or repaired if it is not working properly or its program can be changed. The deployment is randomized and after deployment, the nodes are self configured.

All nodes are GPS enabled and the lifetime of the network is simulated. In a particular iteration, if the path count hits zero, then that message is not delivered to the base station. This is because, the battery energy of the critical nodes (nodes near to the base station.) are very low or zero and these nodes do not have any energy. The sensor nodes are isolated from base station and network collapses. The two algorithms (H-SPREAD and DRFSD) are compared with respect to latency, residual energy and delivery probability.

In the case of H-SPREAD, the network breaks down very fast. This is because the data paths are always in zigzag fashion. The path in some instances moves away from base station and thus increases the overall path length. Hence, the number of transmissions and the propagation energy requirement increases. The nodes consume huge amount of energy and the critical nodes die very soon. The paths reaching the base station decreases with the increase in simulation time and when more nodes die, then there are no paths to the base station and the network breaks down at this state. In the DRFSD approach, the paths are always in the direction of the base station. So the nodes do not spend unnecessary energy in the routing process and the network lifetime increases when compared to H-SPREAD.

Delivery Probability (DP) is the number of packets that reach the base station/sum of packets generated at all nodes. The Delivery probability is shown in the Figure 4. With the passage of time, DP decreases due to increase in link failures. In the H-SPREAD protocol, the total number of packets delivered to the base station reduces due to large link failures. In case of DRFSD, link failures are lower and DP is higher than H-SPREAD.

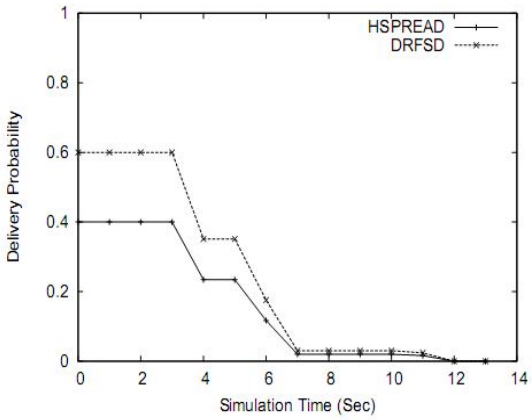

Fig. 4. Delivery Probability in H-SPREAD, DRFSD Algorithms.

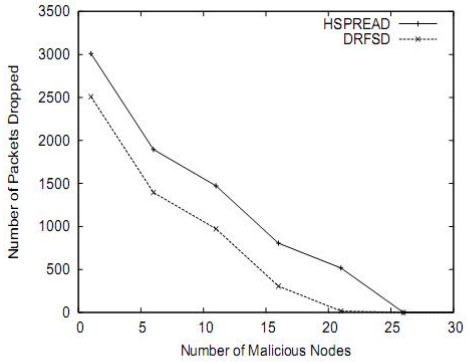

Fig. 5. Path Generated when malicious nodes present in H-SPREAD and DRFSD Algorithm.

Figure 5 depicts the packet drop probability in H-SPREAD, DRFSD. Since the H-SPREAD involves larger number of nodes for transmitting data to the Base Station, it encounters larger number of malicious nodes in its path and hence the number of packet delivered is lower than in DRFSD. Due to smaller of nodes participating in DRFSD, the packet delivery probability is higher in DRFSD protocol.

CONCLUSIONS

Secure routing is a challenging task in Wireless Event Sensor Networks. Existing multipath routing protocols provides security by taking longer distance paths, consuming more energy and incurring high latency.

Hence, the attacker gets sufficient time to hack the data or disturb the network. We have proposed Directed Restricted Flooding for Secure Data-aggregation protocol (DRFSD) which addresses these issues.

In DRFSD, alternate multipaths are selected for data transmission based on 180◦ direction with the Base Station and the number of nodes participating in the transmission phase and distance reduces in comparison with H-SPREAD. Security is enhanced and latency is lower than H-SPREAD. Results show that proposed protocol is better in terms of latency, security, residual energy and delivery probability in comparison with H-SPREAD leading to increased life time.

REFERENCES

[1] Wenjing Lou, Wei Liu and Yuguang Fang, SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks, IEEE INFOCOM, March 2004.

[2] Wenjing Lou and Y. Kwon, H-SPREAD: A Hybrid Mulipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks, IEEE INFOCOM, March 2004.

[3] Wenjing Lou, An Efficinet N-to-1 Multipath Routing Protocol in Wireless Sensor Networks, in Proc. 2nd IEEE Int. Conf. MASS, pp. 665-672, Nov. 2005.

[4] Swades De, Chunming Quia and Hongyi Wu, Meshed Mutipath Routing with Selective Forwarding: An Efficient Strategy in Wireless Sensor Networks, Computer Networks, Elsevier, pp. 481-497, 43 (2003).

[5] Chris Karlof and David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Ad Hoc Networks, Elsevier, vol. 1, no. 2-3, pp. 293-315, Sept. 2003.

[6] Reza Curmola and Cristina Nita-Totaru, ”BSMR: Byzantine-Resilient Secure Multicast Routing in Multi hop Wireless Networks,” IEEE Transactions on Vehicular Technology, vol. 55, no. 4, pp. 1320-1330, July-2006.

[7] Min-Ho Park, Young-Hoon Park, Han-YounJeong and Seung-Woo Seo,” Secure Multiple Multicast Services in Wireless Networks,” IEEE Transactions on Mobile Computing, vol. 12, no. 9, pp. 1712-1723, September-2013.

[8] Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhing Chen and Xuemin Shen, ”Secure and Energy-Efficient Disjpoint Multipath Routing for WSNs,” IEEE Transactions on Vehicular Technology, vol. 16, no. 7, pp. 3255-3265, September-2012.

[9] P. Karunakaran and C. Venkatesh, ”Traffic and Security using Randomized Dispersive Routes in Heterogeneous Sensor Networks,” International Journal of Distributed and Parallel Systems (IJDPS) , vol. 3, no.1, pp. 219-228, January-2012.

[10] Salman-ul-Hassan D., Zoya T., Fatima M. and Umer I.,” GPS-Based Landmine Detection System for Multiple Operating Units,” IEEE, International Conference on Robotics and Artificial Intelligence (ICRAI), 2012.

[11] Ravindra Gupta and Hema Dhadhal, ”Secure Multipath Routing in Wireless Sensor Networks,” International Journal of Electronics and Computer Science Engineering (IJECSE), vol. 1, no. 2, pp. 585-589, 2012.

[12] Shancang Li, Shanshan Z., Xinheng W., Kewang Z. and Ling Li,” Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks,” IEEE Systems Journal, vol. 24, no. 5, pp. 1-10, February-2013.

[13] Hannes Frey, ”Lower and Upper Bounds for Multicasting under Distance Dependent Forwarding Cost Functions,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 5, pp. 963-976, May-2013.

[14] Sankardas Roy, Mauro Conti, Mauro Conti and Sushil Jajodia,” Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attackers Impact,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 681-694, April-2014.

[15] Ing-Ray Chen, Fenye Bao, MoonJeong Chang and Jin-Hee Cho, ”Dynamic Trust Management for Delay Tolerant Networks and its Application to Secure Routing,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, pp. 1200-1210, May-2014.

★★★