Journal of Computer Science 8 (2): 232-238, 2012
ISSN 1549-3636


# Secure Authentication Technique for Data Aggregation in Wireless Sensor Networks

[1]Bhoopathy, V. and [2]R.M.S. Parvathi
[1]Department of CSE,
Annai Mathammal Sheela Engineering College, Tamil Nadu, India
[2]Department of CSE,
Sengunthar College of Engineering, Tamil Nadu, India

**Abstract: Problem statement:** In Wireless Sensor Networks (WSN), serious security threat is caused by node capture attacks where an adversary gains full control over a sensor node through direct physical access. **Approach:** This creates a high risk of data confidentiality. **Results:** We propose a secure authentication technique for data aggregation in WSN. During first round of data aggregation, the aggregator upon identifying the detecting nodes selects a set of nodes randomly and broadcast a unique value which contains their authentication keys, to the selected set of nodes. When any node within the set wants to send the data, it sends slices of data to other nodes in that set, encrypted with their respective authentication keys. Each receiving node decrypts, sums up the slices and sends the encrypted data to the aggregator. **Conclusion/Recommendations:** The aggregator aggregates and encrypts the data with the shared secret key of the sink and forwards it to the sink. In the second round of aggregation, the set of nodes is reselected with new set of authentication keys. By simulation results, we show that the proposed approach rectifies the security threat of node capture attacks.

**Key words:** Wireless Sensor Networks (WSN), group based key management protocol (DGKE), Robust Authentication Scheme (RAS), Cooperative Distributed Detection (CDD), Simple Distributed Detection (SDD), Distributed Coordination Function (DCF)

## INTRODUCTION

**Wireless sensor networks:** Wireless sensor networks comprises of the upcoming technology that has attained noteworthy consideration from the research community. Sensor networks comprise of many small, low cost devices and are naturally self organizing ad hoc systems. The function of the sensor network is monitoring the physical environment, collect and transmit the information to other sink nodes. In general the range of the radio transmission for the sensor networks are in the orders of the magnitude which is smaller than the geographical extent of the intact network. Hence, the data has to be transmitted hop-by-hop towards the sink in a multi-hop manner. The consumption of energy in the network can be reduced if the amount of data to be relayed is reduced (Vass and Vidacs, 2007).

Wireless sensor network comprises of a great number of minute electromechanical sensor devices which posses the sensing, computing and communication abilities. These devices can be utilized for gathering sensory information, like measurement of temperature from an extended geographical area (Kohonen, 2004).

Many of the features of the wireless sensor networks give rise to challenging problems (Hartl and Li, 2004). The most important three characteristics are:

- Sensor nodes are the ones which are prone to maximum failures
- Sensor nodes make use of the broadcast communication pattern and have severe bandwidth restraint
- Sensor nodes have limited amount of resources

**Data aggregation:** Data aggregation is considered as one of the fundamental distributed data processing procedures for saving the energy and minimizing the medium access layer contention in wireless sensor networks (Zhenzhen *et al*., 2007). Data aggregation is presented as an important pattern for routing in the wireless sensor networks. The basic idea is to merge the data from various sources, reroute it with the elimination of the redundancy and thus reducing the number of transmissions and saving the energy (Krishnamachari *et al*., 2002). The inbuilt redundancy

**Corresponding Author:** Bhoopathy, V., Department of CSE, Annai Mathammal Sheela Engineering College, Tamil Nadu, India

in the raw data gathered from various sensors can be prevented by the in-network data aggregation. Additionally, these operations use raw materials for obtaining application specific information. To preserve the energy in the system for maintaining longer lifetime in the network, it is important for the network to maintain high incidence of the in-network data aggregation (Fan *et al*., 2007).

**Secure data aggregation:** The issues related to the security in the data aggregation of WSN are as follows (Sang *et al*., 2006).

**Data confidentiality:** In particular, the basic security issue is the data confidentiality which safeguards the transmitted data that is sensitive from passive attacks like eavesdropping. The importance of the data confidentiality is in the hostile environment, where the wireless channel is more susceptible to eavesdropping. Even though cryptography has provided plenty of methods, the operation related to complicated encryption and decryption, like modular multiplication of large numbers in public key based cryptosystems, uses the sensor's power quickly.

**Data integrity:** It prevents the alteration of the final aggregation value by the compromised source nodes or aggregator nodes. Sensor nodes can be easily compromised due to the lacking of the expensive tampering-resistant hardware. The otherwise used hardware may not be reliable at times. A compromised message is capable of modifying, forging and discarding the messages.

In general, for secure data aggregation in wireless sensor networks, two methods can be used. They are hop by hop encrypted data aggregation and end to end encrypted data aggregation (Sang *et al*., 2006).

**Hop-by-Hop encrypted data aggregation:** In this technique, the encryption of the data is performed by the sensing nodes and decryption by the aggregator nodes. The aggregator nodes aggregate the data and again encrypt the aggregation result. At the end, the sink node on obtaining the final encrypted aggregation result decrypts it.

**End to End encrypted data aggregation:** In this technique, the aggregator nodes in between have no decryption keys and can only perform aggregation on the encrypted data.

**Node capture attacks:** The process of getting hold of the sensor node through a physical attack is termed as node capture attack. For example: uncovering the sensor and adding wires in any place. This attack essentially differs from getting hold of a sensor via certain software bug. Since sensors are typically supposed to operate the same software, specifically, the operating software which discovers the suitable bug permits the adversary to manage the entire sensor network. Distinctly, the node capture attacks can be set over a small segment of adequately large network (Benenson *et al*., 2005).

## MATERIAL AND METHODS

The blend of passive, active and physical attacks by an intellectual adversary results in node capture attack. The adversary initializes an attack by gathering the data's about WSN by overhearing something on message exchanges. This is performed either locally to single adversarial device or via entire network with the help of several adversarial devices organized in the entire network. Along with passive learning, the adversary dynamically takes part in network protocols, inquiring the network regarding the information and injecting malicious information in the network.

The adversary performs the physical attacks, following active and passive learning. To enhance the function of the attack related to certain attack objective, the gathered information can be utilized to aid the adversary in choosing the sensor node (Tague and Poovendran, 2008).

There are two types of node captures possible:

- Random node capture
- Selective node capture

The above node captures varies in the key distribution information to the attacker. The attacker should minimum capture hundreds of sensor nodes during selective node capture attacks (Ren *et al*., 2008).

**Problem identification:** In sensor node compromise technique, there is a initiation of node capture attack where the adversary physically captures the sensor nodes, removes them, compromises and redeploys them in the network. Following the redeployment of the compromised nodes, it builds up a variety of attacks through compromised nodes. The forceful attacker weakens the sensor network protocols along with the formation of clusters, routing and data aggregation and hence resulting in recurrent disruption of network operations. Therefore, the node capture attacks are unsafe and need to be identified as soon as possible for reducing the damages caused by them (Ho, 2010).

During the node capture attacks, the adversary attempts to tamper the node physically for extracting the secrets of the cryptography. Based on the security architecture of the network, this type of attack is highly destructive and furthermore results in influential insider attacks.

A security issue of WSN corresponds to node capture attack which leads to compromise in the communication of a whole sensor network (Kifayat *et al*., 2007).

In study (Bhoopathy and Parvathi, 2011), we proposed an Energy Efficient Secure Data Aggregation Protocol or wireless sensor networks. In this protocol, we incorporate the authentication and security to maintain the efficiency of the data aggregation. Whenever a sensor node wants to send data to another node; first the sensor node encrypts the data using a key and sends it to the aggregator. For integrity of the data packet, a MAC based authentication code is used. The security problem of WSN such as node capture attacks is not taken into consideration. This node capture attack is harmful for network communication in network data aggregation, routing and so on.

We propose a secure authentication protocol over node capture attacks in wireless sensor networks.

**Related works:** Kifayat *et al*. (2007) proposed a novel and distinct Structure and Density Independent Group Based Key Management Protocol (DGKE). The protocol offers a better secure communication, secure data aggregation, confidentiality and resilience against node capture and replication attacks using reduced resources. The drawback of this approach is that security issues are not considered which impacts significantly on key management (Hu *et al*., 2007) proposed a Robust Authentication Scheme (RAS) for filtering false data in wireless sensor networks. In RAS, each big event is divided into several small event chunks, every one of which is endorsed by witness nodes both with dynamic authentication tokens from one-way hash chain and their secret keys pre-loaded from the key pool. This way, compromised nodes, even in possession of all endorsement keys for the data reports will not able to fabricate or modify the reports.

Eldefrawy *et al*. (2010) proposed a key distribution protocol based on the public key cryptography. The protocol establishes pairwise keys between nodes according to a specific routing algorithm after deployment, instead of loading full pair-wise keys into each node. The proposed scheme comes to circumvent the shortage of providing the re-keying property of nodes.

Kohno *et al*. (2011) proposed a new method resilient to node capture attacks. This method utilizes secret sharing scheme to disperse confidential information without the need of a secret key. This method is implemented on the motes nodes and it is more effective as the number of hops-to-sink node increases. On the other hand the increased overhead is observed on short hop node. They have also shown a countermeasure capable of reducing excess dispersals without degrading the resilience against node capture attacks.

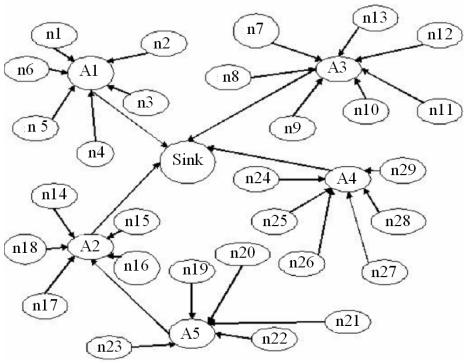


Fig. 1: System Architecture

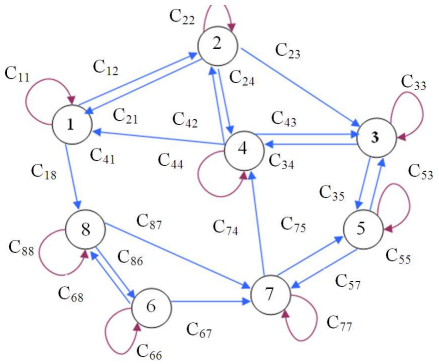


Fig. 2: Slicing architecture (Network size u = 8, Hop length $h_L$ = 1)

Conti *et al*. (2008) proposed two efficient and distributed solutions. In the first proposal, Simple Distributed Detection (SDD), the attack is detected using only information local to the nodes. The second solution, the Cooperative Distributed Detection (CDD), exploits node collaboration to improve the detection performance. CDD outperforms both SSD in a meaningful scenario. Moreover, the proposed solutions do not rely on any specific routing protocol-we only use direct range communications and message flooding.

Hung *et al*. (2009) investigated the effects of different node capture attack patterns on state-of-the-art key management schemes. They proposed two recovery strategies, namely link replacement strategy and node replenishment strategy to replace the compromised region, respectively. This proposed approach achieves significant improvement in terms of network resilience.

**Proposed work:**

**System architecture:**

**Algorithm:** Let $u_i$ represent a member node in cluster $C_j$ (i = 1, 2,….n). Let $A_j$ be the aggregator of the cluster $C_j$. Let $R_1$ represents the first round of aggregation and $TS_1$ represents its respective time stamp. $A_j$ possess a secret key ($k^j_{sec}$) which is shared with the sink (Fig. 1-12).

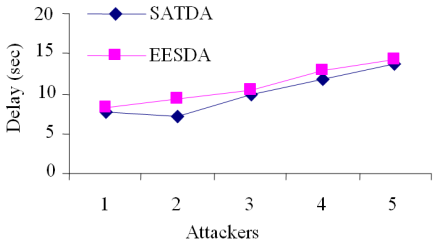


Fig. 3: Attackers Vs delay we can see that the average end-to-end delay of our proposed SATDA protocol is less than the existing EESDA protocol

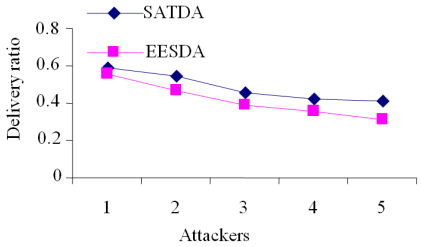


Fig. 4: Attackers Vs delivery ratio we can see that the packet delivery ratio of out proposed SATDA protocol is higher than the existing EESDA protocol

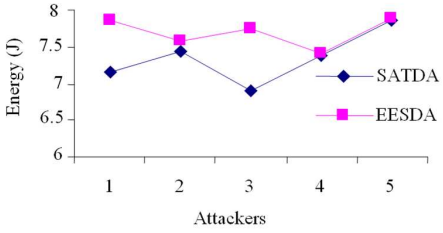


Fig. 5: Attackers Vs Energy we can see that the Energy consumption of our proposed SATDA protocol is less than the existing EESDA protocol

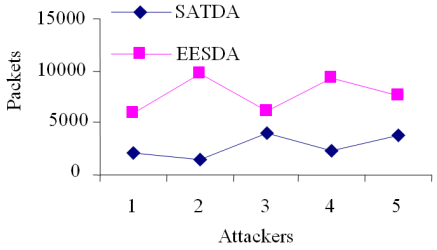


Fig. 6: Attackers Vs drop we can see that Packet drop ratio of our proposed SATDA protocol is less than the EESDA protocol

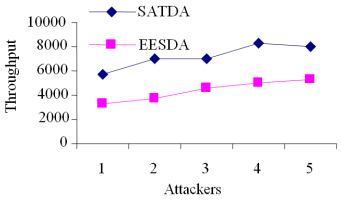


Fig. 7: Attackers Vs throughput we can see that throughput of our proposed SATDA protocol is higher than the existing EESDA protocol

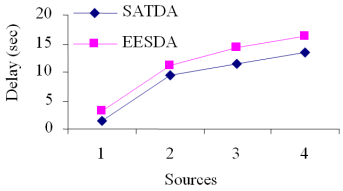


Fig. 8: Sources Vs delay we can see that the average end-to-end delay of our proposed SATDA protocol is less than the existing EESDA protocol

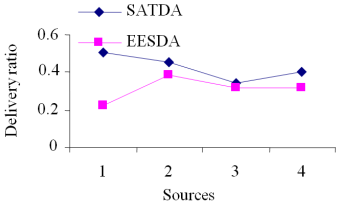


Fig. 9: Sources Vs delivery ratio we can see that the packet delivery ratio of out proposed SATDA protocol is higher than the existing EESDA protocol

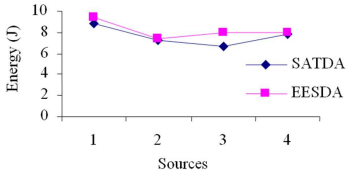


Fig. 10: Sources Vs energy we can see that the Energy consumption of our proposed SATDA protocol is less than the existing EESDA protocol

During $R_1$, the aggregator broadcasts the aggregator advertisement message ($AGG_{adv}$) to all the nodes within a cluster:

$$A_j \xrightarrow{AGGadv} u_i$$

The nodes that receive the $AGG_{adv}$ reply back the aggregator with Acknowledgment (ACK) message:

$$u_i \xrightarrow{ACK} A_j$$

The format of ACK message is:

$$ACK = \{w_i, g\}$$

Where:
$w_i$ = Node's ID
G = Node's category

- Based on the received ACK messages, the aggregator selects c nodes ($c \leq n$) randomly
- The selected c nodes are represented by the set Q = $\{u_1, u_2, \ldots..u_c\}$
- Then, the aggregator broadcasts a set of unique values V to all nodes in Q. V consist of the node ids of Q and their authentication key:
  $V = [(w_1, K_{w1}), (w_2, K_{w2}), \ldots\ldots\ldots, (w_c, K_{wc})]$

Here $K_{wi}$ denotes the authentication keys of the corresponding node $w_i$:

$$A_j \xrightarrow{V} Q$$

The following Table 1 represents a set of unique values V:

- When any node within Q wants to send the data (say X), initially it slices X into c pieces. This slicing technique is described. Among c slices, one of them is kept inside that node itself. The remaining (c-1) pieces are sent to all nodes in Q by encrypting the pieces with their corresponding authentication keys (given in Table 1
- When a node receives the encrypted slice, it performs the decryption of that slice using its shared authentication key (given in Table 2). Upon receiving the first slice, the node waits for a time t, which assures that all slices of this round of aggregation are received
- When the node decrypts all the received slices, it sums them up including the slices within the node (say $c_{ii}$) and the sum is represented as $S_c$. $S_c$ is again encrypted with the authentication key of the respective node and sent to the aggregator $A_j$
- $A_j$ aggregates and encrypts the data with the shared key $k^j_{sec}$ and forwards it to towards sink. The forwarded message to the sink will be in the form MAC (ED, $TS_1$)

$TS_1$ = Time stamp

Table 1: Set of unique value V

| Node ID | Authentication key |
|---|---|
| $w_1$ | $K_{w1}$ |
| $w_2$ | $K_{w2}$ |
| $w_3$ | $K_{w3}$ |
| . | . |
| . | . |
| $w_c$ | $K_{wc}$ |

Table 2: Represents the flow of data slices among nodes and its related authentication keys

| Sender node | Receiver node | Data slice | Authentication key |
|---|---|---|---|
| 1 | 2, 8 | $c_{12}$, $c_{18}$ | $k_2$, $k_8$ |
| 2 | 1, 3, 4 | $c_{21}$, $c_{23}$, $c_{24}$ | $k_1$, $k_3$, $k_4$ |
| 3 | 4, 5 | $c_{34}$, $c_{35}$ | $k_4$, $k_5$ |
| 4 | 1, 2, 3 | $c_{41}$, $c_{42}$, $c_{43}$ | $k_1$, $k_2$, $k_3$ |
| 5 | 3, 7 | $c_{53}$, $c_{57}$ | $k_3$, $k_7$ |
| 6 | 7, 8 | $c_{67}$, $c_{68}$ | $k_7$, $k_8$ |
| 7 | 4, 5 | $c_{74}$, $c_{75}$ | $k_4$, $k_5$ |
| 8 | 6, 7 | $c_{86}$, $c_{87}$ | $k_6$, $k_7$ |

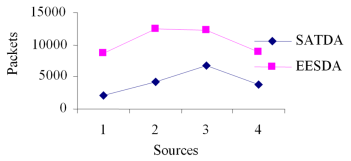


Fig. 11: Sources Vs drop we can see that Packet drop ratio of our proposed SATDA protocol is less than the EESDA protocol

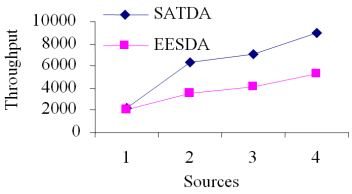


Fig. 12: Sources Vs throughput we can see that throughput of our proposed SATDA protocol is higher than the existing EESDA protocol

ED = Encrypted data

$$A_j \xrightarrow{MAC(ED,TS)} Sink$$

- If $TS_1$ expires, session $R_1$ ends and the second round of aggregation ($R_2$) with the time stamp ($TS_2$) begins
- The same procedure is repeated for $R_2$ except that the set of nodes in Q is reselected with new set of authentication keys

**Slicing technique:** Consider the node 2 in Fig. 2. When it wants to send data to its neighboring nodes, it slices the data (X) into 8 pieces (since network size u = 8). It holds the one of the slices with it. The remaining slices are encrypted with their respective authentication keys and sent to rest of the nodes.

When the node 1 receives the encrypted data slice from node 2, it decrypts the slice using its authentication key $K_1$. Then Node 1 waits for reception of the rest of the slices until time t. When t expires, the node 1 stops receiving the data slice. After complete decryption of the received slices, the node 1 sums them up along with the slice within it and this sum is represented as $S_1$:

$$S_1 = c_{11} + c_{21} + c_{41}$$

Similarly the summed data of other nodes are as follows:

$S_2 = c_{12} + c_{22} + c_{42}$

$S_3 = c_{23} + c_{33} + c_{43} + c_{53}$

$S_4 = c_{24} + c_{44} + c_{74} + c_{34}$

$S_5 = c_{75} + c_{35} + c_{55}$

$S_6 = c_{66} + c_{86}$

$S7 = c_{67} + c_{87} + c_{57} + c_{77}$

$S_8 = c_{88} + c_{68} + c_{18}$

The node 1 encrypts $S_1$ with $k_1$ and sent to the aggregator $A_1$. The aggregator encrypts the data with the secret shared key ($k^j_{sec}$) and forwards it to the sink.

Advantages of this approach:

- The set of nodes selected during the slicing process varies session after session. The sliced encrypted data send to the nodes will be visible to those nodes and attacker finds it difficult to disclose the information as it varies for every round of aggregation. Thus slicing technique enables the secure authentication over node capture attacks
- Since the data slices are encrypted with authentication keys, even if one slice is attacked, remaining slices stay secured. And thus an attack does not have much impact on the forwarded data's
- When the end-to-end communications are encrypted, the intermediate nodes could not easily perform in-network processing to get aggregated results. And even during link level encryption, the privacy is violated. Thus the slice blended aggregation enables reduced communication overhead

## RESULTS AND DISCUSSION

**Simulation setup:** The performance of our SATDA protocol is evaluated through Network Simulator Version-2 Ns-2 (Network Simulator: www.isi.edu/nsnam/ns) simulation. A random network deployed in an area of 351×351 m is considered. Initially 30 sensor nodes are placed in square grid area by placing each sensor in a 50×50 grid cell. 4 phenomenon nodes which move across the grid (speed 5m $sec^{-1}$) are deployed to trigger the events. 4 aggregators are deployed in the grid region according to our protocol. The sink is assumed to be situated 100 meters away from the above specified area. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The Distributed Coordination Function (DCF) of IEEE 802.11 is used for wireless LANs as the MAC layer protocol. The simulated traffic is CBR with UDP source and sink. The number of sources is fixed as 4 around a phenomenon. Table 3 summarizes the simulation parameters used.

**Performance metrics:** The performance of Secure Authentication Technique for Data Aggregation (SATDA) protocol is compared with our previous work Energy Efficient Secured Data Aggregation (EESDA) protocol (Bhoopathy and Parvathi, 2011). The performance is evaluated mainly, according to the following metrics:

**Average end-to-end delay:** The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations

**Average packet delivery ratio:** It is the ratio of the number of packets received successfully and the total number of packets transmitted.

**Average energy:** It is the average energy consumption of all nodes in sending, receiving and forward operations.

**Average packet loss:** It is the average number of packet dropped at each receiver.

**Throughput:** It is the number of packets successfully received by the receiver

**Based on attackers:** In our initial experiment, we vary the number of attackers as 1-5.

Table 3: Simulation Parameters

| No. of nodes | 30 |
|---|---|
| Area size | 351×351 |
| Mac | 802.11 |
| Routing protocol | DSDV |
| Simulation time | 50 sec |
| Traffic source | CBR |
| Packet size | 50 bytes |
| Rate | 50 bytes |
| Transmission range | 150 m |
| No. of events | 4 |
| No. of sources | 1, 2, 3 and 4 |
| No. of attackers | 1,2,3,4 and 5 |
| Speed of events | 5 m $sec^{-1}$ |

## CONCLUSION

In this study, we have proposed a secure authentication technique for data aggregation in WSN. During first round of data aggregation, the aggregator upon identifying the detecting nodes selects a set of nodes randomly and broadcast a unique value which contains their authentication keys, to the selected set of nodes. When any node within the set wants to send the data, it sends slices of data to other nodes in that set, encrypted with their respective authentication keys. Each receiving node decrypts, sums up the slices and sends the encrypted data to the aggregator. The aggregator aggregates and encrypts the data with the shared secret key of the sink and forwards it to the sink. In the second round of aggregation, the set of nodes is reselected with new set of authentication keys. By simulation results, we have shown that the proposed approach rectifies the security threat of node capture attacks.

## REFERENCES


Benenson, Z., N. Gedicke and O. Raivio, 2005. Realizing robust user authentication in sensor networks. RWTH Aachen University.

Bhoopathy, V. and R.M.S Parvathi, 2011. Energy efficient secure data aggregation protocol for wireless sensor networks. Eur. J. Sci. Res, 50: 48-58.

Conti, M., R.D. Pietro, L.V. Mancini and A. Mei, 2008. Emergent properties: Detection of the node-capture attack in mobile wireless sensor networks. Proceedings of the 1st ACM Conference on Wireless Network Security, (WNS' 08), ACM New York, USA., pp: 214-219. DOI: 10.1145/1352533.1352568

Eldefrawy, M.H., M.K. Khan and K. Alghathbar, 2010. A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. Proceedings of the International Conference on Anti-Counterfeiting Security Identification Communication, Jul. 18-20, IEEE Xplore Press, Chengdu, pp: 1-6. DOI: 10.1109/ICASID.2010.5551480

Hartl, G. and B. Li, 2004. Loss inference in wireless sensor networks based on data aggregation. Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Apr. 26-27, ACM, New York, USA., pp: 396-404. DOI: 10.1145/984622.984680

Ho, J.W., 2010. Distributed detection of node capture attacks in wireless sensor networks. Smart Wireless Sensor Netw.

Fan, K.W., S. Liu and P. Sinha, 2007. Structure-free data aggregation in sensor networks. IEEE Trans. Mobile Comput., 6: 929-942. DOI: 10.1109/TMC.2007.1011

Hung, K.S., C.F. Law, K.S. Lui and Y.K. Kwok, 2009. On attack-resilient wireless sensor networks with novel recovery strategies. Proceedings of the IEEE Wireless Communications and Networking Conference, Apr. 5-8, IEEE Explore Press, Budapest, pp: 1-6. DOI: 10.1109/WCNC.2009.4917842

Kifayat, K., M. Merabti, Q. Shi and D. Llewellyn-Jones, 2007. Group based secure communication for large-scale wireless sensor networks. Liverpool John Moores University, UK.

Kohno, E. and T. Ohta, Y. Kakuda and M. Aida, 2011. Improvement of dependability against node capture attacks for wireless sensor networks. IEICE Trans. Inform. Syst., E94: 19-26.

Kohonen, J., 2004. Data Gathering in sensor networks. Helsinki Institute for Information Technology, Finland.

Krishnamachari, L., D. Estrin and S. Wicker, 2002. The impact of data aggregation in wireless sensor networks. Proceedings of the 22nd International Conference on Distributed Computing Systems, Jul. 5-5, IEEE Explore Press, pp: 575-578. DOI: 10.1109/ICDCSW.2002.1030829

Ren, K., W. Lou and Y. Zhang, 2008. LEDS: Providing location-aware end-to-end data security in wireless sensor networks. IEEE Trans. Mobile Comput., 7: 585-598. DOI: 10.1109/TMC.2007.70753

Sang, Y., H. Shen, Y. Inoguchi, Y. Tan and N. Xiong, 2006. Secure data aggregation in wireless sensor networks: A survey. Proceedings of the International Conference on Parallel and Distributed Computing, Applications and Technologies, Dec. 4-7, IEEE Xplore Press, Taipei, pp: 315-320. DOI: 10.1109/PDCAT.2006.96

Tague, P. and R. Poovendran, 2008. Modeling node capture attacks in wireless sensor networks. Proceedings of the 46th Annual Allerton Conference on Communication, Control and Computing, Sep. 23-26, IEEE Explore Press, Urbana-Champaign, IL, pp: 1221-1224. DOI: 10.1109/ALLERTON.2008.4797699

Vass, D. and A. Vidacs, 2007. Distributed Data Agregation with Geographical Routing in Wireless Sensor Networks. Proceedings of the IEEE International Conference on Pervasive Services, Jul. 15-20, IEEE Explore Press, Istanbul, pp: 68-71. DOI: 10.1109/PERSER.2007.4283891

Hu, Y., Y. Lin, Y. Liu and W. Zeng, 2007. RAS: A Robust Authentication Scheme for Filtering False Data in Wireless Sensor Networks. Proceedings of the 15th IEEE International Conference on Networks, Nov. 19-21, IEEE Explore Press, Adelaide, SA, pp: 200-205. DOI: 10.1109/ICON.2007.4444086

Zhenzhen, Y., A.A. Abouzeid and A. Jing, 2007. Optimal policies for distributed data aggregation in wireless sensor networks. Proceedings of the 26th IEEE International Conference on Computer Communications, May 6-12, IEEE Explore Press, Anchorage, AK, pp: 1676-1684. DOI: 10.1109/INFCOM.2007.196