A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks

Neeraj Kumar[1], Manoj Kumar[1], and R. B. Patel[2]
(Corresponding author: Neeraj Kumar)
School of Computer Science and Engineering, SMVD University, Katra (J&K), India[1]
Department of Computer Science and Engineering, MM University, Mullana (Ambala), Haryana, India[2]
(Email: nehra04@yahoo.co.in)
(Received Aug. 27, 2009; revised and accepted Jan. 23, 2010)

Abstract

Data dissemination is important concept in wireless sensor networks (WSN). In this paper, we propose a secure and energy efficient data dissemination protocol for WSN. A routing metric is defined to choose the best route from the available routes. This metric guides those routes to be chosen that consume less energy. Moreover, for secure data dissemination, a session key is established between different parties to be communicated. This session key is then used for secure communication among nodes for data dissemination. The performance of proposed protocol is evaluated using NS-2 simulator with respect to the metrics like control overhead, network lifetime, and throughput. It is found that the proposed protocol is quite effective in comparison to the existing protocols with respect to these metrics.

Keywords: Data dissemination, energy efficiency, routing, wireless sensor network

1 Introduction

Wireless Sensor networks (WSNs) are drawing much attention in the research community over the years due to wide variety of applications. To deploy sensor networks in a particular region, security is an important aspect and should be provided against various attacks such as node capture, physical tempering, denial of service, etc. [22, 37, 44]. When embedded in critical applications, WSNs are likely to be attacked [23, 44].

One of the major concerns in WSNs applications is the design and development of a secure and energy-efficient routing protocol. In this regard, consuming low power and increasing networks lifetime [2] are two important attributes of any secure routing protocol for WSN, i.e., the protocol should ensure that connectivity in the network is maintained for longer duration, and the energy status of the entire network should be of the same order. This is in contrast to energy optimizing protocols that find optimal paths and then consume the energy of the nodes along those paths, leaving the network with a wide disparity in the energy levels of the nodes, and eventually disconnected. If nodes in the network consume energy equally, then the nodes in the center of the network continue to provide connectivity for longer duration.

It is therefore crucial to provide energy efficient security solutions to WSNs. The critical issue one needs to tackle when using existing methods to secure a network is the key distribution, which has been intensively studied recently (e.g., [3, 5, 6, 11, 12, 14, 18, 19, 20, 21, 27, 28, 29, 38, 39, 47, 48]) in the context of WSNs. Cluster-based organization (e.g., [16, 46]) has been proposed for WSNs. In cluster-based networks, nodes are typically organized into clusters, with cluster heads (CHs) relaying messages from ordinary nodes in the cluster to the base stations (BSs). Clustered WSNs were first proposed for various reasons including scalability and energy efficiency while performing data aggregation.

In this paper, we propose a Secure and Energy Efficient Data Dissemination protocol for WSN. The protocol operates in two phases namely as establishment of session key and data dissemination with hop-by-hop authentication. For data dissemination and energy saving, we have defined the routing metric which is included in the route reply and route request packet for selection of best available routes.

Rest of the paper is organized as follows: Section 2 discusses the related work, Section 3 defines the models used along with the defined routing metric, Section 4 describes the proposed solution, Section 5 provides the simulation and results obtained, and finally Section 6 concludes the article.

2 Related Work

Wood and Stankovic [44] surveyed a number of denial of service (DOS) attacks in WSNs, and discussed some possible countermeasures. Karlof and Wagner [23] focused on routing layer attacks, and showed how some of the existing WSN protocols are vulnerable to these attacks. Cryptographic solutions [3, 5, 6, 11, 12, 14, 18, 19, 20, 21, 27, 28, 29, 38, 39, 47, 48]), have focused on efficient key management of symmetric schemes without tying them to a particular network organization. Balakrsihnan et al. [16], propose an energy efficient mechanism for WSN. By using elliptic curve cryptography [4, 15, 24, 30, 46], it has been shown that sensor nodes are indeed able to compute public key operations. However, public key authentication in the context of WSNs is still an open problem, as they cannot afford a conventional public key infrastructure and the proposed alternatives [13] are not applicable to all contexts.

Perrig et al. [36], proposed SPINS. SPINS includes two efficient symmetric key based security building blocks: SNEP and μTESLA. SNEP provides confidentiality, authentication, and freshness between nodes and the BS, and μTESLA provides authenticated broadcast. Nidal Nasser et al. [32], proposed a secure and energy-efficient multipath routing protocol for wireless sensor networks called SEEM. It uses multipaths for communication between two nodes thus prolongs the lifetime of the whole network. On the other hand, SEEM is effectively resistive to some specific attacks that have the character of pulling all traffic through the malicious nodes by advertising an attractive route to the destination.

Zhu et al. [49], proposed an interleaved hop-by-hop authentication scheme to prevent injection of false data into sensor networks. The proposal makes sure that the BS can detect a false report when no more than a certain number of nodes are compromised. Przydatek et al. [40], proposed SIA, a framework for secure information aggregation in WSNs which makes use of random sampling strategies for allowing user to infer about the legitimacy of a value. Other efforts have focused on more specific types of attacks. Hu et al. [17], studied and offer solutions for wormhole attacks, whereas Newsome et al. [34], investigated sybil attacks in the context of WSNs. Deng et al. [9], address secure in-network processing, and propose a collection of mechanisms for delegating trust to aggregators. The mechanisms address both dissemination and aggregation of data. Yea et al. [45], proposed SEF, a statistical en-route filtering mechanism for detecting and dropping bogus reports while being forwarded. It allows both the BS and the en-route nodes to detect false data with a certain probability. Neeraj et al. [33], also propose an agent based secure location aware key establishment scheme in WSN. Landstra et al. [25] propose an energy efficient hybrid key management protocol for WSNs. Dressler [10] proposed an authenticated Reliable and Semi-reliable Communication in WSNs. Das [8] presents an identity-based random key pre-distribution scheme for direct key establishment to prevent attacks in wireless sensor networks. Agah and Das [1] present DOS attack with respect to game theory approach in WSNs. Soliman and Omari [41] present a dynamic encryption system for WSNs. Liang et al. [43] present node failure of tolerance in WSNs. Mohaisen et al. [31] present a hierarchical pair wise key establishment in WSNs. Das [7] presents a location aware key establishment scheme for WSNs.

3 Models and Routing Metrics

3.1 Network Model

The proposed network model is shown in Figure 1. There are three types of nodes considered in this Figure: BS, CH and sensor nodes. BS is the most powerful and overall in charge of the network, because it has maximum resources in terms of energy. In this model, we consider a network of heterogeneous and energy-constrained sensor nodes that are randomly deployed in a sensor field. Sensor nodes are initially powered by batteries with full capacities. Each sensor collects data which are typically correlated with other sensors in its vicinity. As shown in figure, each sensor nodes send their data to BS via CHs to save energy. The nodes with dark circle are considered as CH while with light circle are considered as sensor nodes. CHs communicate with each other and sensor nodes to collect the data and then send it to BS. We assume periodic sensing with the same period for all sensors and CH is elected as in [35]. Inside each fixed cluster, a node is periodically elected to act as CH through which communication to/from cluster takes place [35].

3.2 Energy Model

To ascertain the amount of energy consumed by a radio transceiver, we apply the following energy model. For each packet transmitted by a sending node to one or more receivers in its neighborhood, the energy is calculated as according to [16]:

$$e = e_t + ne_r + (N-n)e_r^h,$$

where e_t and e_r denote the amount of energy required to send and receive, n is the number of nodes which should receive the packet, and N the total number of neighbors in the transmission range. quantifies the amount of energy required to decode only the packet header According to model described in [16], e_t and e_r are defined as

$$\begin{aligned} e_t(d,k) &= (e_{elect} + e_{amp} * d^{\rho})8k; \\ e_r(k) &= e_{elect} * 8k. \end{aligned}$$

For a distance d and a k byte message. We have set

$$e_{elect} = 70nJ/bit, e_{amp} = 120pJ/bit/m^2, d = 50m, \rho = 4.$$

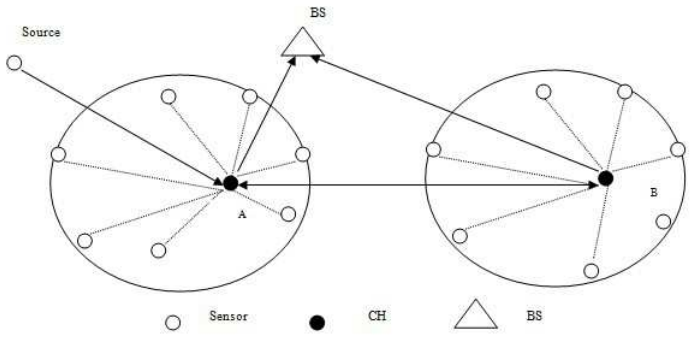

Figure 1: Data transmission in typical sensor networks

3.3 Routing Metric

The cost of a link between two sensor nodes S_i and S_j is equal to the energy spent by these nodes to transmit and to receive one data packet, successfully. To establish the coverage and connectivity aware connection between two sensors, a proper routing metric is needed which will guide to form the connection between the sensors. The following routing metric (R_metric) is proposed and is calculated as follows:

$$R_metric = \langle \frac{E_i^D}{E_t(S_i, S_j) + E_r(S_i, S_j)} \rangle,$$

where E_i^D is energy associated with the delivery ratio of the packet originating from source node and correctly received at destination node, while $E_t(S_i, S_j)$ is the energy used in transmitting from S_i to S_j and $E_r(S_i, S_j)$ is the energy used in receiving the packet.

3.4 Threat Model and Security Goals

We assume that following type of inside attacks that can occur on the network:

- The adversary has the ability to capture a legitimate node and turn it into a malicious node, which is to extract cryptographic keys from a captured node and to make malicious code run for the attacker's purpose.
- A compromised node can launch selective forwarding attacks (malicious nodes arbitrarily drop the relaying packets instead of forwarding them). Even if the adversary is able to compromise a legitimate node, it fails to replicate the captured node indefinitely with the same ID and spread them over the network.
- The adversary could inject malicious routing information that leads to routing inconsistencies. During routing advertisements a compromised node can advertise forged routing information. Also attacker tunnels packets from one location to another location in the network called wormhole attack Moreover sinkhole attack can also be dangerous for WSN.

Following security goals are considered in the proposed approach:

- To defend against the various types of attacks like sinkhole, wormhole, selective forwarding and reply attack.
- Secure and energy efficient data dissemination from source to destination for high throughput and packet delivery fraction.
- Efficient data dissemination without additional overhead on the network.

4 Proposed Solution

The proposed approach for secure (with respect to the above defined threat model) and energy efficient data dissemination in WSN consists of two phases namely as:

Establishing the session key and data dissemination with hop-by-hop authentication. Each phase is explained by its respective algorithm. The session key is established dynamically by the participating nodes in that session. Each sensor node is assigned a unique identification (ID), a node specific key (K_i), and common key K. Two cluster heads $(CH)_A$ and $(CH)_B$ are considered for establishing the session key.

4.1 Establishing the Session Key

Any sensor node initiates the session set-up procedure by transmitting a set-up request packet (Figure 2). Request to establish a session key goes to their respective CH node. Let the node S in $(CH)_A$ starts the procedure as follows:

$$\begin{aligned} S &\rightarrow (CH)_A : RREQ \\ RREQ &\rightarrow ((Request_ID)_s.(seession_ID)_{old}, R\_metric, \\ &\quad info, h\_c, MAC(K_A, (ID)_A, (session_ID)_{old}, \\ &\quad traffic_info)), \end{aligned} \quad (1)$$

where $Request\_ID$ is the identification of the request, if the request is to re-establish a previously broken session,

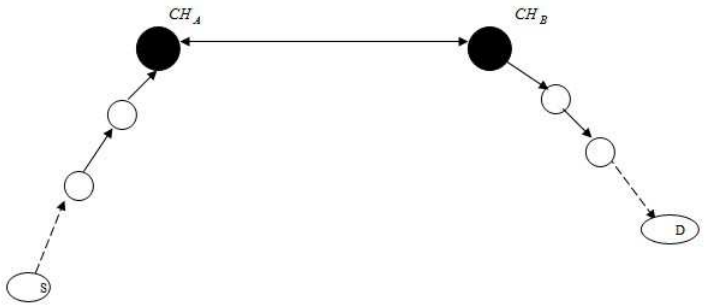

Figure 2: Establishment of session key in the proposed approach

the identification of the broken session is $(session\_ID)_{old}$, R_metric defines the routing metric between the nodes, $traffic\_info$ is used for information about the traffic to be sent, h_c is the hop count starting from source node(S) and message authentication code (MAC) [produced using the key which the CH shares with the BS].

Every intermediating forwarding node (say j) checks $traffic info$. If node j decides to forward the packets in this connection, it computes the MAC which will be used by the BS for the purpose of authentication on the request it received from the previous forwarding node, $j-1$ by using its own secret key, replaces the MAC in the request and forwards $RREQ$ to the next intermediate node as:

$$RREQ_j \rightarrow ((Request_ID)_j, (seession_ID)_{old}, R\_metric, traffic\_info, h\_c, MAC(K_j, RREQ_{j-1}). \quad (2)$$

The request delivered to $(CH)_A$ contains MAC computed by $(CH)_A$ and all the forwarding nodes. $(CH)_A$ repeats all the MAC computations and checks the result against the MAC in the received request. It also verifies that the $Request_ID$ is fresh. This procedure authenticates all the nodes in the route and cluster head A. If verifications is not successful, $(CH)_A$ drops the request. Otherwise, it sends the request to $(CH)_S$.

Processing at cluster head B:
When $(CH)_B$ receives the request, it forwards it to the first node to be sent to Destination (D).

$$\begin{aligned} (CH)_B &\rightarrow D : RREQ \\ RREQ &\rightarrow ((Request\_ID)_D, (session\_ID)_{old}, R\_metric, traffic\_info, h\_c. \end{aligned}$$

$(Request\_ID)_D$ is a fresh identifier generated by $(CH)_B$. Similar to Phase 1, every node l to D also checks $traffic\_info$ to decide if it wants to get involved in this session, generates a new MAC and replaces the existing MAC in the $RREQ_{i-1}$ before forwarding it to D.

$$RREQ_{-1} \rightarrow ((Request\_ID)_D, (session\_ID)_{old}, R\_metric, traffic\_info, h\_c, MAC(K_{l-1}, RREQ_{-l-1}).$$

When D receives the request, and if it accepts this connection, it prepares the reply and sends it back. The reply contains only $(ID)_D$ and MAC, which was generated on the overall message forwarded to $(CH)_B$ by the last node as follows:

$$RREP \rightarrow ((ID)_D, MAC(K_D DREQ_{D-1}). \quad (3)$$

$RREP$ is conveyed back to $(CH)_B$ through the same route without any modification. Then $(CH)_B$ generates the MAC for the route and verifies it with the returned MAC. If the verification does not fail, then it informs $(CH)_A$. Now both $(CH)A$ and $(CH)_B$ generate confirmation messages $conf_S$ and $conf_D$ respectively and send them to S and D as follows:

$$\begin{aligned} (CH)_S\_Conf &= ((Request\_ID), (Session\_ID), MAC_S(K_i, S_{ID}, (Session\_ID)_S, (Session\_ID)_{old}, R\_metric, traffic\_info, h\_c). \end{aligned}$$

$$\begin{aligned} (CH)_D\_Conf &= ((Request\_ID), (Session\_ID)_{old}, MAC_D(K_i, D_{ID}, (Session\_ID)_D, (Session\_ID)_{old}, R\_metric, traffic\_info, h\_c). \end{aligned}$$

Each node on the route verifies its own MAC and stores session identification accordingly. So a session key is to be establishing before any data is to be sent between S and D. This session key is broadcasted by the respective cluster heads to their nodes before sending any data to their respective cluster heads. Also R_metric is calculated at each transmission so that effective paths can be chosen for session establishment. This session key is generated dynamically keeping in view of the dynamic nature of the network.

4.2 Data Dissemination

In each session, each CH broadcast a new session key obtained by the above procedure using the public key K.

After session key is established, data dissemination phase begins as follows:

Step 1. If sensor node i wants to send the data to its CH, go to next step else exit the algorithm.

Step 2. Sensor node i requests the respective CH to send the current session key established during the Section 4.1. This key is broadcasted using the public key K in encrypted form as $E_k(K_s)$, where K_s is the session key.

Step 3. Sensor node i, XOR the current session key K_s with predefined key K_i to compute $K_{i,s}$.

Step 4. Sensor node i encrypt the data with $K_{i,s}$ and attach its own ID, and MAC($K_{i,s}$, $Data$) to send it to CH using those paths that have minimum value of R_metric.

Step 5. CH receives the data, attach its own ID, and the send to higher level CHs or BS.

Step 6. BS decrypts the data using key established in Section 4.1.

Step 7. Check the data freshness by h_c and calculate the MAC to verify its integrity.

Step 8. If the data is altered or replayed, then discard the data, go to Step 10.

Step 9. Decide whether to request all sensor nodes for retransmission, go to step1 else go to Step 10.

Step 10. Ask the respective nodes to transmit the data again.

Steps (1-3) are used for the generation of fresh session key with predefined and generated session key in Section 4.1. This is used to check the freshness of the session key. In Step 4, minimum energy path is chosen using Equations (1, 2, 3) to send the encrypted data to respective CHs to save energy during transmission. For each path, R_{metric}, is calculated from S to D and minimum value is chosen. Steps (5-7) are used by respective CHs to decrypt the data and checks its integrity using MAC and h_c. Step 8 is used to check the authenticity of the data. Steps (9-10) are used for retransmission of the data if the data is altered in the path.

Hop-by-Hop Verification for Sinkhole attack:
In the proposed scheme, nodes with wrong information are detected and excluded from the network by hop-by-hop verification system.

1) During a route setup phase, any neighboring node receiving a suspicious h_c in route update immediately reports the information to BS via CHs.

2) Receiving the report(s), the BS broadcast all the neighboring nodes to report information about the suspect node.

3) All the neighboring nodes of the suspect node report the information about the suspect node to the BS. Collecting the reports from the neighbor nodes, the BS decides whether the suspect node is actually compromised, or not.

4) The BS revokes the entire key of the compromised node(s) by broadcasting the whole network so that the node is excluded from the network. The procedure for hop-by-hop authentication is as follows:
When a node S accesses the network for the first time or needs a token for neighbor verification, it requests the token from the trusted party like CHs. It is assumed that CHs are secured and they does not involve in any malicious activity. The CH first authenticates the node S and sends a token to it as follows:

$$\begin{aligned} CH &\rightarrow S : Secure_token \\ Secure\_token &= \{(id)_s, h\_c, t, e\}_{K_i}, \end{aligned}$$

where id is the node id, h_c is used for preventing an untrusted h_c in a route update message, t is the time of generation of secure token, and e is the expiry of the token.

Starting node S that has a valid token can start a route discovery for D by broadcasting $RREQ$ packet (the format of the packet is as defined by Equation (2). Each time a route discovery process is completed, value of h_c increments to ensure the freshness of the reply message expected from D. When a node receives a $RREQ$ message, it first decrypts the message and then records the neighbor that sends the message as the next hop node for S of the message. If the node receives a reply message for this $RREQ$, it just forwards the reply to the neighbor in this record. Finally, it encrypts the message by using its private key, appends its secure token to it and broadcasts the message to the next destination.

Also each intermediate node checks the h_c of the message received with the generated h_c of the parent. If the new h_c of the message is less than or equal to the parent h_c, then the message is accepted otherwise it is rejected. So this procedure gives an efficient mechanism for hop-by-hop neighbor verification.

Every intermediate node decrypts the received message, encrypts it again by using its own private key and appends its secure token to the message before forwarding. To decrypt the message a node needs the public key of the neighbor that it receives the message from. That public key is in the secure token appended to the message, which is encrypted by the private key of the CHs. Every node knows the public key of the CH, and secure token issued are encrypted by the CH. Each node authenticates the previous node in the route because messages are signed at each hop. Therefore, malicious nodes do not have the opportunity to redirect traffic by tunnelling or modifying h_c. So this mechanism provides efficient security mechanism for hop-by-hop neighbor verification.

Hence the proposed system is secured with respect to various networks attacks.

4.3 Security Analysis

The proposed scheme can defend against attacks on routing protocols that attract traffic by advertising high quality routes to BS. It also defends the selective forwarding attack, and altering the routing information. For this, the proposed scheme uses ARMS [26] and the proposed hop-by-hop neighbor verification system for authentication (defined in Section 4.3)of sensor node's route advertisements. ARMS prevents a routing message from being spoofed and altered, by means of a one-time key MAC scheme. Also, the sequence number S_i in the route update is a defense against replay attacks.

For defense against the Selective forwarding, each node keeps multiple nodes in the routing table and forwards packets through alternate paths to one of its parent node so that packets from descendent nodes of a compromised node have an opportunity to bypass the node which arbitrarily drops them. Thus, the proposed scheme mitigates the effect of selective forwarding nodes by trying to bypass them.

Also the sinkhole attack is defended by means of hop-by-hop neighbor verification system as defined in Section 4.3.

5 Simulation and Results

We have evaluated the performance of the proposed protocol by simulation using NS-2 [42]. We consider a rectangular region of area $100 \times 100m$, in which the wireless sensor nodes are deployed in an ad hoc manner. There is one BS to which all the sensor nodes in the network need to send their data packets. The transmission range of each node is 20 m. We have compared the performance of proposed protocol with SEEM [32]. Each simulation experiment was conducted using 10 different network topologies, and each result was averaged over 10 runs of different network topologies.

The performance of the designed protocol is compared under two conditions: normal conditions and conditions with 50% of malicious nodes. The performance of the designed protocol is measured by the number of sensor nodes blocked by a set of compromised nodes in each round by increasing the number of compromised nodes in the network. The following key parameters are measured during the simulation run:

Throughput. This is the percentage of successfully received data packets by BS.

Control Overhead. Control overhead is defined as the ratio of control packets (Route Discovery, Route Discovery Reply, Neighbor Collection, Data dissemination Enquiry, and Data dissemination Reply) to data transmissions.

Network Lifetime. The lifetime of the network is defined as the time at which the first node failure occurs, i.e., the time at which some node's energy reserve is reduced to zero. The lifetime of a WSN is directly linked to the energy consumption of each node.

Node Resilience. The node tolerance power after the attack occurs on the network.

Figures 3, 4, 5 show the performance comparison of SEEM [32] and proposed protocol when there is no attack on the network. From the figures, we can observe that both SEEM and proposed scheme have a high packet delivery ratio which increases as the number of nodes increases. Both SEEM and proposed schemes select an optimal path from a number of choices. The proposed scheme chooses the best path depending upon R_metric defined in Section 2. Also control overhead increases as the size of the network increases. This is due to the fact that both BS and sensor nodes need to flood control packets to the whole network. When the nodes density increases each node has more neighbors and more control packets are sent and received between neighbors. However the control overhead is less in the proposed scheme than SEEM due to the fact that proposed scheme chooses the best available path dynamically by using R_metric. Moreover only the session key is required to authenticate the data to be sent to the respective nodes, while node id is used for public key of each node.

Also network lifetime increases than SEEM considerably. R_metric in the proposed scheme is adaptive in nature and choose the best available path so that less energy can be consumed which has a direct effect on the network lifetime. This is due to the fact that all the previous proposed schemes use the same path for all communications between the source and BS. The direct consequence of this is that nodes on this particular path may deplete energy very soon. But in the proposed scheme, the CH selects a new path with minimum value of R_metric. With this dynamic path selection mechanism, the CH ensures that it can select the most optimal path for data dissemination.

Figures 6, 7, and 8 show the results when 50% of nodes are malicious. The throughput does not decrease in both protocols. When malicious nodes are on the routing path and do not forward packets for the source, the proposed scheme can detect this behavior as explained in Section 4.3 in which various types of attacks can be defended using existing techniques.

Node Resilience:
In the presence of 50% of the compromised nodes (almost 100 nodes out of 200 nodes taken) which drop all the relaying packets and advertise inconsistent routing information, the effect of proposed scheme on a ratio of blocked nodes is shown in Figure 9. Without the proposed scheme, the influence of compromised nodes over the network is more since compromised nodes even attract the network traffic and drop them. Using proposed scheme, however,

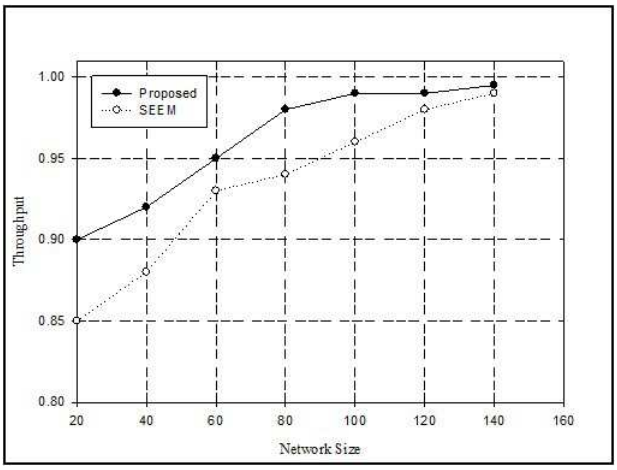

Figure 3: Throughput in SEEM and proposed scheme

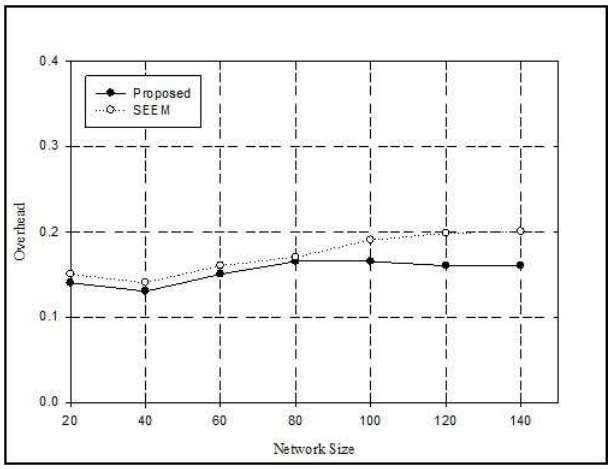

Figure 4: Control overhead in SEEM and proposed scheme

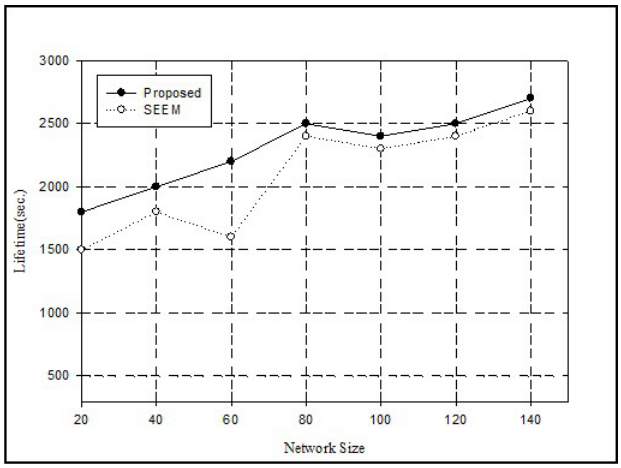

Figure 5: Network lifetime in SEEM and proposed scheme

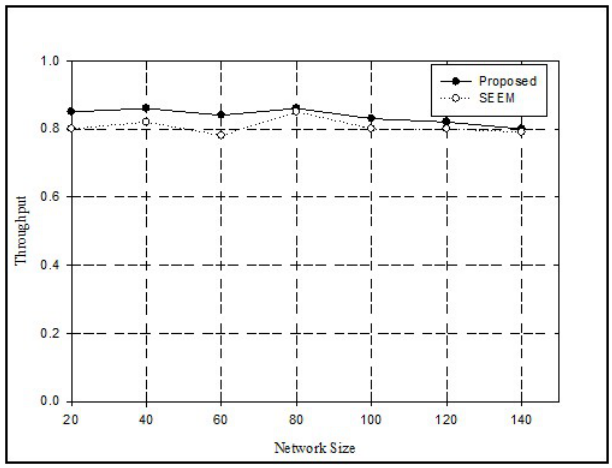

Figure 6: Throughput in SEEM and proposed scheme when the nodes are malicious

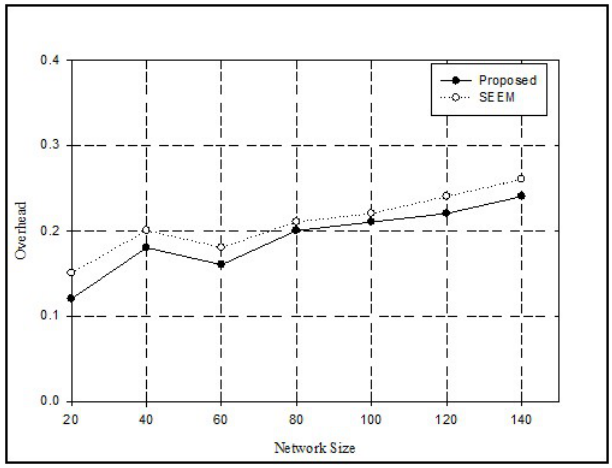

Figure 7: Control overhead in SEEM and proposed scheme when the nodes are malicious

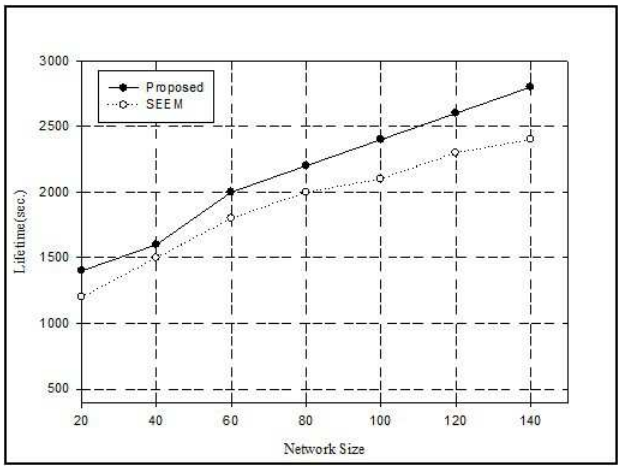

Figure 8: Network lifetime in SEEM and proposed scheme when the nodes are malicious

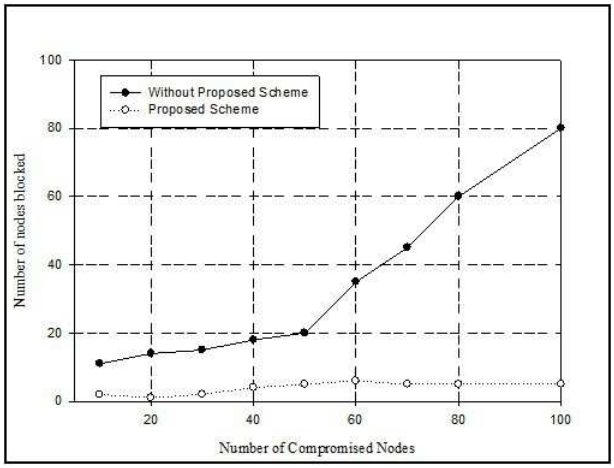

Figure 9: Node Resilience against node capture attack in the proposed scheme and without proposed scheme

we can see that more than 90% of sensor nodes are not blocked.

Legitimate nodes did not forward packets to the compromised nodes identified. Thus, with several compromised nodes, almost all of them are excluded from the network so that more than 90% of sensor nodes are not blocked.

Also the routing path is selected by the respective CH, which periodically re-selects a new path according to R_metric defined in Equation 1 along multipaths. Therefore, whatever the compromised node advertises, it has no impact on routing path and cannot attract traffic through itself. Even if the compromised nodes are happened to be in the routing path, the attack lasts only for limited period. Hence the proposed scheme is quite effective against the wormhole and sinkhole attack.

6 Conclusions

In this paper, we propose a secure and energy efficient protocol for WSNs. Compared to other proposed routing protocols, the proposed scheme considers security and energy-efficiency. A new routing metric is defined based upon which the optimal path is chosen. The session key is used by the CH to pass the information to BS. The lifetime of the whole network is increased by using multipath to transfer data along with reducing the delay by using the shortest and reliable path. Moreover the proposed scheme is resistant to various types of attacks. Hence the proposed scheme can be applicable for wide variety of applications.

References

[1] A. Agah, and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145-153, 2007.

[2] K. Akkaya, and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325-349, 2005.

[3] S. A. C. Amtepe, and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *9th European Symposium on Research Computer Security (ESORCS' 04)*, *Lecture Notes in Computer Science*, pp. 293-308, Sophia Antipolis, France, Sep. 2004.

[4] E. O. BlaX, and M. Zitterbart, "Towards acceptable public-key encryption in sensor networks," *The 2nd International Workshop on Ubiquitous Computing*, ACM SIGMIS, May 2005.

[5] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," *IEEE Symposium on Security and Privacy (S&P'03)*, pp. 197-213, May 2003.

[6] H. Chan, and A. Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," *The 24th Conference of the IEEE Communications Society (INFOCOM' 05)*, Mar. 2005.

[7] A. K. Das, "ECPKS: An improved location-aware key management scheme in static sensor networks," *International Journal of Network Security*, vol. 7, no. 3, pp. 358-369, 2008.

[8] A. K. Das, "An identity-ased random key predistribution scheme for direct key establishment to prevent attacks in wireless sensor networks," *International Journal of Network Security*, vol. 6, no. 2, 134-144, 2008.

[9] J. Deng, R. Han, and S. Mishra, "Security support for in-network processing in wireless sensor networks," *1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03)*, pp. 83-93, ACM Press, New York, 2003.

[10] F. Dressler, "Authenticated reliable and semi-reliable communication in wireless sensor networks," *International Journal of Network Security*, vol. 7, no. 1, pp. 61-68, 2008.

[11] W. Du, J. Deng, Y.S.H.S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," *Conference of the IEEE Communications Society (INFOCOM' 04)*, 2004.

[12] W. Du, J. Deng, Y.S. Han, P.K. Varshney, and J. Katz, A. Khalili, A pairwise key pre-distribution scheme for wireless sensor networks, *ACM Transactions on Information Systems and Security*, vol. 8, no. 2, pp. 228-258, 2005.

[13] W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," *6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, pp. 58-67, ACM Press, NY, USA, 2005.

[14] L. Eschenauer, and V. D. Gligor, "A key management scheme for distributed sensor networks," *9th ACM Conference on Computer and Communications Security (CCS' 02)*, pp. 41-47, ACM New York, 2002.

[15] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bitcpus," *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 119-132, Cambridge, MA, USA, 2004.

[16] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," *IEEE Hawaii International Conference on System Sciences*, pp. 4-7, Jan. 2000.

[17] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless sensor networks," *Conference of the IEEE Communications Society (INFOCOM' 03)*, 2003.

[18] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," *2nd ACM International Conference on Wireless Sensor Networks and Applications (WSNA' 03)*, pp. 141-150, ACM Press, New York, 2003.

[19] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN' 04)*, *ACM Press*, pp. 29-42, New York, 2004.

[20] J. Hwang, and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 43-52, ACM Press, New York, 2004.

[21] R. Kannan, L. Ray, and A. Durresi, "Efficient key pre-distribution schemes for sensor networks," *1st European Workshop on Security in Wireless and Ad-Hoc Sensor Networks (ESAS' 04)*, Heidelberg, Germany, Aug. 2004.

[22] C. Karlof, and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113- 127, May 2003.

[23] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293-315, 2003.

[24] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics and Computation*, vol. 48, pp. 203-209, 1987.

[25] T. Landstra, S. Jagannathan, and M. Zawodniok, "Energy efficient hybrid key management protocol for WSNs," *International Journal of Network Security*, vol. 9, no. 2, pp. 121-134, 2009.

[26] S. B. Lee, and Y.-H. Choi, "ARMS: An authenticated routing message in sensor networks," *Secure Mobile Ad-hoc Networks and Sensors Workshop (MADNES'05)*, Springer-Verlag, Sep. 2005.

[27] D. Liu, and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks," *10th Annual Network and Distributed Systems Security Symposium (NDSS'03)*, pp. 263-276, 2003.

[28] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions Information Systems Security*, vol. 8, no. 1, pp. 41-77, 2005.

[29] D. Liu, and P. Ning, "Location-based pairwise key establishments for static sensor networks," *1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03)*, pp. 72-82, ACM Press, New York, 2003.

[30] V. Miller, "Uses of elliptic curves in cryptography," *Advances in cryptology, Crypto'85*, LNCS 218, vol. 218, pp. 417-426, Springer-Verlag, Berlin, 1986.

[31] A. Mohaisen, D. Nyang, and K. Lee, "Hierarchical grid-based pairwise key pre-distribution in wireless sensor networks," *International Journal of Network Security*, vol. 8, no. 3, pp. 282-292, 2009.

[32] N. Nasser, and Y. Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks," *Computer Communications*, vol. 30, pp. 2401-2412, 2007.

[33] N. Nehra, and R. Patel, "MASLKE: Mobile agent based secure location aware key establishment in wireless sensor networks," *proceedings of 16th IEEE International conference on networks (ICON 08)*, pp. 12-14, New Delhi, Dec. 2008.

[34] J. Newsome, R. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis and defenses," *IEEE International Conference on Information Processing in Sensor Networks (IPSN 2004)*, Apr. 2004.

[35] R. B. Patel, T. S. Aseri, and D. Kumar, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," *Computer Communications*, vol. 32, no. 4, pp. 662-667, Mar. 2009.

[36] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521-534, 2002.

[37] A. Perriig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.

[38] R. D. Pietro, and L. V. Mancini, and A. Mei, "Random key-assignment for secure wireless sensor networks," *SASN '03: of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 62-71, New York, USA, 2003.

[39] R. D. Pietro, L. V. Mancini, and A. Mei, "Efficient and resilient key discovery based on pseudo-random key pre-deployment," *Wireless Networks*, vol. 12, no. 6, 2006.

[40] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," *ACM SenSys 2003*, Nov. 2003.

[41] H. S. Soliman, and M. Omari, "Application of Synchronous Dynamic Encryption System (SDES) in wireless sensor networks," *International Journal of Network Security*, vol. 3, no. 2, pp. 160-171, 2006.

[42] The network Simulator, NS2. (http://www.isi.edu/nsnam/ns/)

[43] L. M. Wang, J.-F. Ma, and Y.-B. Guo, "Node-failure Tolerance of Topology in Wireless Sensor Networks," *International Journal of Network Security*, vol. 7, no. 2, pp. 261-264, 2008.

[44] A. D. Wood, and J.A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54-62, 2002.

[45] F. Yea, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *Conference of the IEEE Communications Society (INFOCOM'04)*, 2004.

[46] O. Younis, and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: a hybrid, energy-efficient approach," *Conference of the IEEE Communications Society (INFOCOM' 04)*, pp. 629-640, 2004.

[47] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," *10th ACM Conference on Computer and Communication Security*, pp. 62-72, ACM Press, New York, 2003.

[48] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," *11th IEEE International Conference on Network Protocols (ICNP'03)*, pp. 326-335, Atlanta, Nov. 2003.

[49] S. Zhu, S. Setia, and S. Jajodia, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," *IEEE Symposium on Security and Privacy*, pp. 259-271, 2004.

Neeraj Kumar received his Ph.D. (Computer Science and Engineering) from SMVD Universtity, Katra (J&K), India. He is working as Assistant Professor (School of Computer Science and Engineering), Shri Mata Vaishno Devi University, Katra(India) since 2007. Prior to joining SMVDU, Katra he has worked with HEC Jagadhri and MMEC Mullana, Ambala, Haryana, India as Lecturer. He has published 25 research papers in international journals and conferences of IEEE and Springer. His research is focused on use of agents, mobile computing, parallel/distributed computing, adhoc, sensor and wireless mesh networks, mulit-channel scheduling, resource allocation, multiagent system and fault tolerance. He is a senior member of ACEEE, senior member of IACSIT.

Manoj Kumar is working as Assistant Professor (School of CSE, SMVD University, Katra, J&K, India) since 2008. Prior to joining SMVDU, Katra, he has served in MMU, Mullana (Ambala). He has received his M.Tech.(Computer Science and Engineering) from KU, Kurukshetra (Haryana) and B.Tech.(Computer Science and Engineering) from MMU, Mullana (Haryana).

R. B. Patel received Ph.D from IIT Roorkee in Computer Science & Engineering, PDF from Highest Institute of Education, Science & Technology (HIEST), Athens, Greece, MS (Software Systems) from BITS Pilani and B. E. in Computer Engineering from M. M. M. Engineering College, Gorakhpur, UP. Dr. Patel is in teaching and Research & Development since 1991. He has published about 50 research papers in International/National Journals and Refereed International Conferences. He has been awarded for Best Research paper by Technology Transfer, Colorado, Springs, USA, for his security concept provided for mobile agents on open network in 2003. He has written 5 books for engineering courses. He is member of various International Technical Societies such as IEEE-USA, Elsevier-USA, Technology, Knowledge & Society-Australia, WSEAS, Athens, etc for reviewing the research paper. His current research interests are in Mobile & Distributed Computing, Mobile Agent Security and Fault Tolerance, development infrastructure for mobile & peer-to-peer computing, Device and Computation Management, Cluster Computing, etc.