Secure Protocol for Wireless Sensor Network

Vinay Kumar Pandey
Assistant Prof. CSE, Sat Kabir Institute of Tech. & Mgmt. Haryana, INDIA
Email Id:vkp1979@gmail.com

Gaurav Gupta
Assistant Prof. CSE
RIT Roorkee, INDIA
Email Id:gaurav4584@gmail.com

Sorabh Gupta
Assistant Prof. ECE, COER, Roorkee, INDIA
Email Id:saur72006@yahoo.co.in

***Abstract -Wireless sensor network is an emerging technology due to its wide range of application .This scheme proposes a new secure protocol with better security and Even-driven cluster formation brings energy efficiency by avoiding the unnecessary formation of clusters, when no event is there in the network The proposed scheme adopts a level based secure hierarchical approach to maintain the energy efficiency. It incorporates light-weight security mechanisms like, nested hash based message authentication codes (HMAC), Elliptic-Curve Diffie-Hellman (ECDH) key exchange scheme and Blowfish symmetric cipher*.**

Keywords - Wireless Sensor Network, Data Aggregation, Energy Efficiency, Network Lifetime

I. INTRODUCTION

A wireless sensor network (WSM) of distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity.

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

Several advancements are made in securing the wireless communications; wireless sensor network still faces a number of intricacies with respect to secure data transmission. Insecure nature of the radio links, presence of malicious nodes, network jamming and repeating messages are the major problems in wireless sensor network. The three main prerequisites of secure data transmission are: privacy, authenticity and integrity of the transmitted data. The advent of efficient short range radio communication and advances in miniaturization of computing devices have given rise to strong interest in wireless sensor networks [1]. A wireless sensor network (WSN) consists of hundreds or thousands of MEMS-based sensor nodes with the ability to communicate to the external world via base station either directly (single hop) or via other nodes (multi hop) around it in a cooperative manner.

The SHRP scheme proposes a secure hierarchical routing to route the information of devastating events to the base station in a secure energy efficient way. This scheme adopts light-weight security mechanisms like one-way-hash chains (OHC) for authentication purpose, hash-based Message Authentication Codes (HMAC) for authentication and verification of integrity of the messages, Elliptic-Curve Diffie-Hellman (ECDH) key exchange scheme and symmetric key cryptography (Blowfish) [3] for confidentiality. The proposed protocol focuses on securing both the upstream and downstream flow of data. Detection of malicious nodes and sidestepping most of the common attacks on wireless sensor network are the main goals of SHRP.

The secure hierarchical routing protocols have several pros and cons. The main drawback of existing protocols is that more stress is given on securing the upstream flow of data packets. Some of the secure routing protocols overlook the energy constraints [2]. The secure hierarchical routing protocols have several pros and cons. The main drawback of existing protocols is that more stress is given on securing the upstream flow of data packets. [4] .On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks proposes a security solution for a homogeneous network like LEACH [5] where the clusters are formed dynamically and periodically. This security protocol concentrates only on the avoidance of outsider's attack and assumes the base station to be trust worthy. A Key Management Scheme for Cluster Based Wireless Sensor Networks [6] uses public key management scheme based on ECC [7] and Diffie-Hellman [8] key exchange scheme. A low cost ECDSA signature is used for the broadcast authentication of the gateways. Encryption and decryption of messages exchanged between the gateways and the sensor nodes is done using the public key of the gateways. In FBSR, feedback of the current computing capacity from neighboring nodes serves as dynamic information of the current network. This helps in decision making of which nodes will take part in the routing in a secured and energy efficient manner. The feedback from the base station is utilized to identify the malicious nodes. This scheme is well protected against sinkhole attack, selective forwarding and Sybil attack. ATSR calculates the trust value of a node on the basis of multiple attributes like packet forwarding, network layer acknowledgements, message

978-9-3805-4416-8/15/$31.00 ©2015 IEEE

integrity, node authentication etc. Monitoring these attributes help in recognizing various misbehaviors of the nodes and help in avoiding certain attacks.

II. PROPOSED WORK

The proposed scheme SHRP is divided into five modules namely: level formation, cluster formation, key set up, data sensing and aggregation, and routing of aggregated data to the base station

A. Level Formation

In the level formation module the base station broadcasts a request message (REQ) for initiating level formation, to the nodes within two-hop distance, the format of which is:

BS = REQ||BS||OHC||MAC (Gk; REQ||OHC)

A One-way Hash Chain (OHC) is used to authenticate the base station to the nodes of the network.

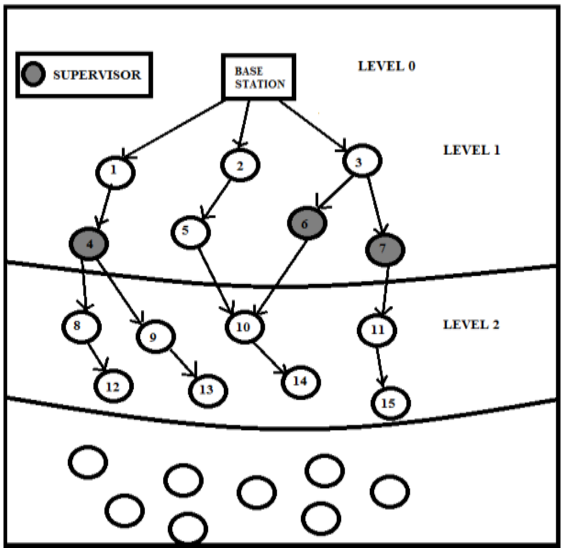

Fig. 1 Level Formation

A hash chain is a sequence of keys generated using a hash function F(x), such that, y=F(x) can be calculated easily and x=$F^{-1(}$y) is computationally infeasible to generate within a finite time. BS is the id of the base station. A MAC is generated on the REQ using the global key Gk, the base station id and the OHC to verify the authenticity of the message and prevent it from being eavesdropped. The hash chain is generated in the order:
Sn→Sn-1→…→S4 →S3→ S2→ S1→ S0.
Base station first uses S1, then S2 and so on.
Once a sequence number is used it is not reused in the lifetime of the network. The request is be verified by MAC generation and OHC computation by the receiving nodes. The request will be acceptable when the output of F (F (…F (Si))) =S0, i.e., by itimes execution of the function F(x) on Si will be S0. The nodes accepting the request will be included in level one. The base station being at level zero acts as the SUPERVISOR which work to monitor the behavior of nodes of next level and assigning trust value to them. If a node forwards less than 30% of the messages, it is marked as a suspicious node.The status value (Stat (i)) is calculated as

Stat (i) =ER (i)*Nng*TV (i)

WhereER(i) is the remaining energy of that node, Nng is the number of neighbor nodes of the next level it can sense and TV(i) is the current trust value of the node. Each node i of level one replace the id of the base station in the request with its own id before forwarding it. A nested MAC is generated over the received MAC from the base station using the global key (Gk), ID of the sender and the OHC. The nested MAC acts as a countermeasure against wormhole attack. The node forwarding the request, also append the status value of itself with the request. The format of the request is:

node(i) = REQ||Stat (i); ||ID (i)||OHC||MAC (Gk; ID;||OHC||(MAC of parent)

The nodes receiving the request of level formation from the nodes of level one mark themselves as nodes of level two and the sender as their parent. Each node of level two selects its SUPERVISOR from the nodes of level one, within its sensing region, on the basis of the Stati value of the forwarding nodes. Thus there are more supervisors at each level

B. Cluster Formation

In the cluster formation phase, SHRP introduces energy efficiency by adopting an event-based cluster formation scheme, where the node that first senses the occurrence of an event initiates the cluster formation. This initiator node broadcasts request for cluster formation to the nodes of the same level at a two hop distance. The format of the request packet is:

Initiator(i)=Clus_REQ||ID(i)||Tv(i)||MAC (Gk;Clus_REQ||ID(i)||Tv(i)

WhereClus_REQ is the request for cluster formation, ID(i) is the ID of the initiator node and TV(i) is the current trust value of the initiator. A node joins the cluster if it receives the request. In case, two nodes sense the event at the same time, the node with higher residual energy will act as the initiator.
Now each node of the cluster calculates a competition bid value for itself. The competition bid is calculated as:

CV(i)= (ER(i)*TV(i)*Nadj) /Davg

Where ER (i) is the remaining energy of the node i, TV (i) is the current trust value, Nadj is the number of nodes in the cluster adjacent to the node and Davg is the average distance of node i from all its adjacent nodes in the cluster.

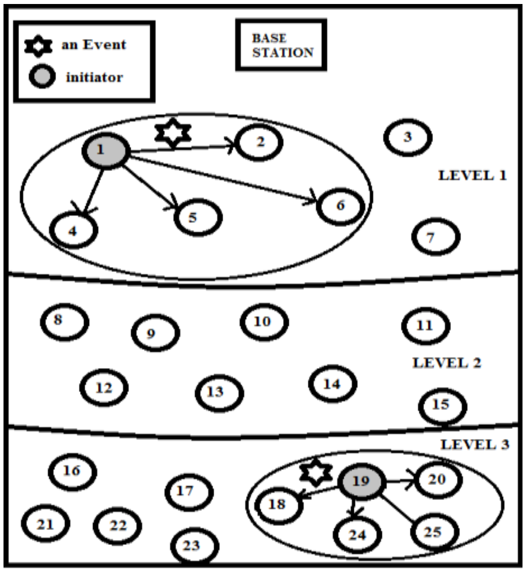

Fig. 2 Cluster Formation

The cluster head of a cluster takes up the role of SUPERVISOR in this phase and periodically monitors the member nodes to assign them their current trust value. The member node with the highest trust value in turn supervises the cluster head to assign its current trust value, at a particular interval. This both-way monitoringavoids assuming any of the nodes in a cluster to be trusted.

C. Key Set up

The next phase is key set up phase. Each cluster head requests a session key from the base station. The request packet is forwarded to the base station following a route in which the next-hop node from the next lower level is chosen on the basis of a weight value Wt. The weight value is calculated as-
Wt= (TV(i)* ER(i))/d(ij)
Wheredij is the distance between the sender and the receiver.
The packet format is:

$$CH(i) = BS{:}key\_REQ||ID_{ch(i)}||TV(i)||MAC\ (Gk;key\_REQ||ID_{ch(i)}||TV(i))$$

Where Key_REQ is the request for a session key, IDCHi is the ID of the cluster head sending the request and TVi is the trust value of that cluster head. The base station then uses Elliptic Curve Diffi-Hellman (ECDH) [2] key exchange scheme to establish a secure channel with each of the cluster heads separately.The base station forwards the public point to the cluster head in level one, if no cluster head is found in that level; it selects an active node of level one with the highest weight value (Wt). The packet format is:

BS=CH(i):QB||BS||IDch(i)||TV(i)||MAC(Gk;QB||BS||IDCH(i)|| OHC)

If the node that received the public point is not the intended cluster head, then it will forward the packet to the next level, until it reaches the cluster head with IDCHx.The packet format is:

$$CH(1)=CH(1+1){:}Q_B||ID(1)||ID_{CH(1)}||OHC||MAC\ (Gk;ID(1)||ID_{CH(1)}||OHC||MAC\_of\_PARENT)$$

D. Data Sensing and Aggregation

After sensing of data each of the member nodes sends a MAC-ed data to the cluster head. The format of the message sent by each member node to the cluster head is:

v → CHx : Rv||IDv||MAC(Gk;MAC(QCx;Rv||IDv||Cv))

Where Rv is the reading of the member node v, IDv is the id of node v, Cv is a counter value that is incremented each time a new packet is forwarded to the cluster head in order to avoid replay attack. The cluster head then performs data aggregation to remove the redundant data and compress it.

E. Routing of aggregated data to the base station

The last phase is routing. The aggregated and compressed data is then encrypted using the session key KS with the help of Blowfish symmetric cipher [3]. The cluster head sends it to the base station followed by a route, in which the next hop node is selected on the basis of weight values (Wt). The message format is:

CHx → BS: ARGx||IDx||Suspectlist||MAC(Gk; MAC(KS;ARGx||IDCHx||Cx))

Where ARGx is the aggregated and encrypted data from cluster head CHx, IDCHx is the id of that cluster head, KS is the secret session key and Cx is a counter value.

III.PERFORMANCE ANALYSIS AND SIMULATION RESULT

The performance analysis of SHRP can be summed up as in the following—

- In SHRP, the base station uses hash functions like MD5 or SHA-1 to generate a chain of numbers such that Si = F (Si+1) and appends a sequence number to every message it forwards.
- While monitoring the nodes of each level by the SUPERVISORs, the suspicious nodes are detected. Thus Sybil attack can be prevented by avoiding those nodes.
- The event-driven cluster formation, weight value based path selection and rotation of the role of cluster head makes SHRP more energy efficient.
- The compromised nodes will not be able to generate valid MACs as they don't have the global key.
  The counter value in the message tries to avoid replay attack.

- The aggregated data is encrypted with the secret session key, which is sharedonly between the base station and the cluster head.

IV. RESULT

Thus from the above methods and formulas we can conclude with the following graph:

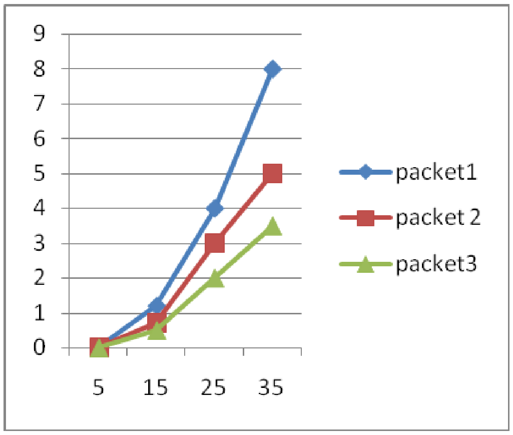

Fig.3

Thus from above method it is clear that Even-driven cluster formation brings energy efficiency by avoiding the unnecessary formation of clusters, when no event is there in the network. Thus, SHRP has better resistance to security threats in wireless sensor network and it can defend well against the different kinds of attacks. Thus, it is also guaranteed from the performance evaluation results that the devastating information sensed by the sensor nodes can reach the base station within a short span of time and also in a secured way. SHRP can prevent attacks like sinkhole, wormhole, Sybil attack, packet eavesdropping and flooding attack.

REFERENCES

[1] A.S. Zahmati, B.Abolhassani, Ali A.B.Shirazi, and A.S. Bahitiari, "An Energy-Efficient Protocol with Static Clustering for Wireless Sensor Networks", International Journal of Electronics, Circuit, and Systems, pp. 135-138, Vol. 1, No. 2, May. 2007.

[2] O. Younis and S. Fahmy, "HEED: A Hybrid Energy-Efficient Distributed Clustering Approach for Ad hoc Sensor Networks", IEEE Transaction on Mobile Computing, pp. 660-669, Vol. 3, No. 4, 2004,

[3] W. R. Heinzelman A. Chandrakasan, and H.Balkrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE Trans. Wireless Communication, pp. 660-670, Vol. 1, No. 4, Oct. 2002.

[4] SoheilGhiasi, Ankur Srivastava, Xiaojian Yang, and Majid Sarrafzadeh, "Optimal Energy Aware Clustering in Sensor Networks", SENSORS Journal, pp. 258-269, Vol. 2, No. 7, 2002.

[5] W.B. Heinzelman et al., An application-specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670.

[6] Reza Azarderakhsh, ArashReyhani-Masoleh, and Zine-EddineAbid, "A Key Management Scheme for Cluster Based Wireless Sensor Networks", In 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.

[7] Asha Rani Mishra and Mahesh Singh, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 3, May 2012.