Secure and Efficient Method of Overcoming Various Attacks in CWSN's

Swathi B R[1]
PG student ,Dept of CSE,
CIT , Gubbi ,
Karnataka ,India

Mr. Anil Kumar G[2]
Associate Prof., Dept of CSE
CIT , Gubbi ,
Karnataka, India

***Abstract*: Wireless Sensor Networks(WSN's) suffer from constraints such as low computation capability, limited energy resources, susceptibility to physical capture, small memory, the use of insecure wireless communication channels and providing security in data transmission. These constraints existing in the network domain makes security in WSN's a challenge. System performance of WSN's is enhanced by using an effective and practical way of introducing clustering technique. A Secure and Efficient data Transmission(SET) expertise for Cluster-based WSN's(CWSN's) called SET-IBS is proposed. SET-IBS expertise uses Identity Based Digital Signature(IBS).The feasibility of SET-IBS expertise is evaluated with respect to security requirements and the security is analyzed against various attacks. In terms of energy consumption and security overhead, the proposed protocol show better performance than existing secure expertise.**

Keywords : Cluster based WSN's, Identity based Digital Signature

I. INTRODUCTION

Wireless Sensor Networks(WSN's) are used in many application such as military, health monitoring and ecological areas, which includes the monitoring and sensitive information such as enemy movement on the battle field or the location of workforce in a building. WSN's provide unforeseen applications in this new fields of design. Operating immense and intricate network requires quantifiability architecture and management strategies. Measurability of sensor nodes can be achieved by using a technique known as clustering where sensor nodes are grouped in different clusters and each clump having a cluster head(CH).Clustering algorithms for sensor networks improves network usage by handling the size and mobility of network. Various clustering algorithms have been proposed, which varies according to overall network. One of the widely used clustering algorithm is LEACH(Low Energy Adaptive Clustering Hierarchy).

In general LEACH protocol effectively reduces and balances the total energy consumption for Clustering-based WSN's(CWSN's) .LEACH achieves refinement in terms of network lifetime. In LEACH-like protocols, network clusters and data links are ranged dynamically, randomly and periodically, which faces a challenge in adding security. The existing protocols symmetric key management for certainty suffers from Orphan node problem[1]. Recently, WSN's provides feasibility by applying asymmetric key management which compensates in terms of security. In asymmetric key management systems, cryptography offers a major critical security services by providing digital signature through a digital certificate. Based on back-breaking of integers factoring from Identity-Based Cryptography(IBC), Identity based digital signatures operates.

II. RELATED WORK

Cluster-based data transmission in WSN's achieves the network usability and management, which enhances the lifetime of sensor node and reduce bandwidth consumption by using local alliance among sensor nodes[3].In a CWSN's, each cluster has a CH and leaf nodes(non-CH sensor nodes).LEACH protocol reduces and balances the total energy consumption for CWSN's. In LEACH protocol, all nodes are assumed to be homogeneous and energy constrained. Cluster member elects the CH to avoid excessive energy consumption.

LEACH protocol consists of two phases namely set-up phase and steady phase, where setup phase includes the process of selecting cluster head and steady phase includes the maintenance of cluster heads by which the data is transmitted between nodes. LEACH protocol assumes that, all nodes are able to reach the sink, but in practical LEACH is suitable only for small size networks. The challenges existing LEACH protocol is that all closer nodes have consistent data, which is not always true and all nodes are continuously listening. By using these existing secure routing protocols it is very difficult to identify the various malicious attacks in the network. LEACH fails to detect those attacks and not able to overcome the attacks in the wireless network channel. In order overcome all these challenges, a Secure and Efficient data Transmission (SET-IBS) protocol is proposed.

III. PROPOSED SYSTEM

The proposed SET-IBS method overcomes the challenges faced by the existing routing protocol such as LEACH protocol. The general network architecture for a cluster-based WSN's is as shown in Fig1, which consists of a fixed base station(BS) and large number of wireless sensor nodes. In CWSN's, all the sensor nodes in the network are grouped into clumps and each clumps has a CH, which is elected autonomously, and leaf sensor nodes. CH aggregates all the data from the leaf nodes and then aggregated data is transmitted for the specified destination.

The proposed SET-IBS method has three steps namely, protocol initialization, key management using IBS scheme and protocol operations. The existing routing protocol such as

AODV, is used to implement the proposed SET-IBS technique forCWSN's.

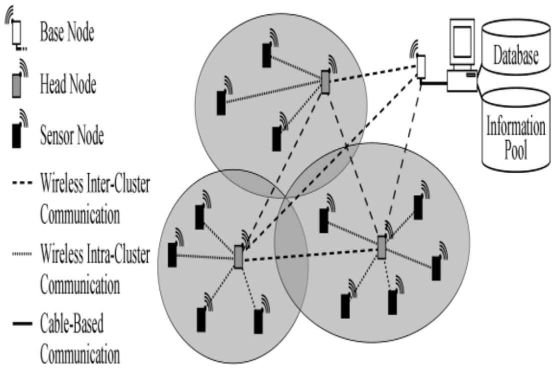
Base Node
Head Node
Sensor Node
Wireless Inter-Cluster Communication
Wireless Intra-Cluster Communication
Cable-Based Communication
Database
Information Pool

Fig1: System Architecture

A. *Protocol Initialization*

Time stamps is maintained in SET-IBS expertise as in case of LEACH-like protocol. Timestamp Ts denotes the timestamps to BS-to-sensor node communication and ti denotes leaf-to-CH communication. In order to improve communication security, key pre-distribution method is adapted. By using IBS scheme, we adapt ID||ti as user public key, corresponding private pairing parameters are pre-loaded into the sensor nodes. In this way, when a node wants to authenticate itself, the node does not have to obtain its private itself at beginning of new round. In case of any node revocation, then BS broadcasts the new compromised node ID's to all nodes, each node then stores revoked ID's within the current round. To provide encryption, we adopt additively homomorphic encryption scheme[4] which guarantees confidentiality.

B. *Key Management Security*

Let us assume that node j transmits a message M and encrypts the data using encryption key K from additively homomorphic encryption scheme. Let C denotes the cipher text of encrypted message. The IBS scheme in proposed SET-IBS consists of following three behaviours:

- *Extraction*: Initially node j acquires its private key
- *Signature signing*: Digital signature is computed on the encrypted message C and then message is broadcasted by concatenating with digital signature.
- *Verification*: Based on the receiving timestamp ti , the sensor generates the complementary digital signature and verifies whether the received message is authentic or not.

C. *Protocol Operation*

The protocol operates in two phases namely setup phase and steady-state phase. In the setup phase, the timestamp Ts and ID's are used for signature generation. In steady-state phase, times stamp ti is used for the signature inception securing the intra cluster communication and Ts is used for signature inception securing CHs to BS transmission.

1)Setup Phase: At the beginning of setup phase of new round, BS broadcasts its ID, nonce and denotation of beginning time Ts of the ongoing round to all cluster members, that is, sensor nodes, which is used later in computing signature and for verification also. Once setup phase is over, network system turns into the steady phase.

2)Steady state phase: Node j transmits the encrypted data C in packets to its CH, which is concatenated with digital signature in a time slot tj , where the sender ID,IDj with tj is the destination identifier for receiver CH. The steady state phase consists of numerous reporting cycles of data transmission from leaf nodes to CHs and is exceedingly long compared to setup phase.

IV. PROTOCOL EVAUATION

In order to evaluate the security of proposed method, three attack models in WSN's are investigated. The attack models are grouped into three categories according to their means of attacks.

1)Passive attack on Wireless channel: Passive attackers performs eavesdropping. They can tackle shipping scrutiny or statistical scrutiny based on monitored or eavesdropped messages.

2)Active attacks on wireless channel: Active attackers tampers the wireless channels. Therefore attackers can forge, reply and modify messages.

3)Node compromising attack: Attackers can physically compromise sensor nodes, and they can access the secret information(secret keys) stored in compromised nodes. Attacks can change the behavior of the compromised sensor nodes.

V. SOLUTIONS TO ATTACKS

In SET-IBS , the encryption of the message provides confidentiality, nonce and time-stamps provide freshness and digital signature provides authenticity and non-repudiation.

1)Solutions to tractable attacks on wireless channel: In SET-IBS, homomorphic encryption scheme encrypts the sensed data. Thus without the decryption keys the unresisting adversaries cannot decipher the eavesdropped message.

2)Solutions to active attacks on Wireless Channel: SET-IBS works well against active attacks in CWSN's. Since attackers do not have digital signature to concatenate with the encrypted message for authentication, attackers cannot pretend as BS or CHs to trigger attackers. Hence SET-IBS are resilient and robust, because CHs being attacked are proficient to disregard all packets with spurious node IDs or spurious digital signature.

3)Solutions to node weaken attacks: In case of node injure attacker, the damage sensor node cannot be assured anymore to fulfill the safety requirements by key managements. Compromised node works normally, but node requires an Intrusion detection expertise to detect and has to replace the node manually or abandon. In order to eliminate compromised sensor node in network, all retracted IDs of damaged nodes will be telecast by BS at beginning of present round. In this way weak nodes can be intercepted from either electing as CHs or consolidating to the clusters in that stage. IBS scheme achieves auxiliary authentication information and message overhead for security can be reduced.

VI. SIMULATION RESULTS

The proposed protocol is evaluated by considering various attacks in WSN's. Three attack models are considered and how security is provided for those attacks is evaluated. The results are obtained from simulations against various attacks. The performance of proposed protocol is evaluated against the performance metric throughput for the different attacks.

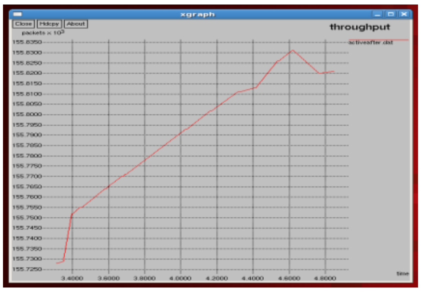

Fig 2 : Throughput achieved when active attack is found in network

The various attacks commonly found in WSN's are discussed in above section. Here we are considering active attack, passive attack, node compromising attacks.Fig 2 shows the throughput achieved by the network when the active attack is found in the network. The simulation is evaluated under various condition and security is analyzed.

Throughput increases exponentially and packet drop is identified. The zigzag curves in the graph shows that there is some attack found in the network. The graph is evaluated against the active attack that is found in wireless network channel. Throughput variation is observed when attack is detected.

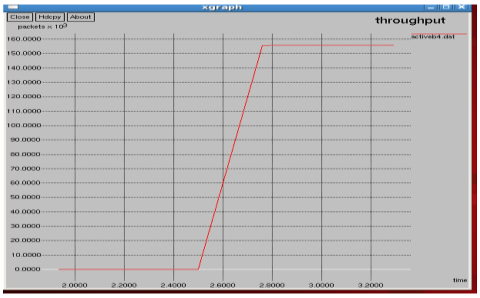

Fig 3:Throughput achieved after overcoming active attack in WSN's

Fig 3 shows the throughput that is achieved by the network channel after overcoming the active attack by using SET-IBS scheme in the wireless network channel. Throughput is constant for some time and then increases rapidly and remains constant, no variation in throughput is observed. Hence throughput can be increased by using the proposed SET-IBS scheme.

VII. CONCLUSION

The proposed SET-IBS expertise achieves feasibility with respect to security requirements and analysis against various attacks. SET-IBS solves the orphan node problem with symmetric key management. The proposed expertise have merits with respect to both reckoning and conveyance costs and evaluated results shows better performance than the existing protocol in CWSN's.

VIII. REFERENCES

[1] S. Sharma and S. K. Jena, “A survey on secure hierarchical routing expertises in wireless sensor networks,” in *Proc. ICCCS*, 2011.

[2] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” in *Lect. Notes. Comput. Sc. - CRYPTO*, 2001

[3] A. A. Abbasi and M. Younis, “A survey on clustering algorithms for wireless sensor networks,” *Comput. Commun.*, vol. 30, no. 14-15, 2007.

[4] C. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient aggregation of encrypted data in wireless sensor networks,” in *Proc. MobiQuitous*, 2005.

[5] S. Xu, Y. Mu, and W. Susilo, “Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security,” in *Lect. Notes. Comput. Sc. - Inf. Secur. Privacy*, 2006.

[6] C.-K. Chu, J. K. Liu, J. Zhou *et al.*, “Practical ID-based encryption for wireless sensor network,” in *Proc. ACM ASIACCS*, 2010.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, “Design and Implementation Issues of Clustering in Wireless Sensor Networks,” *Int. J. Comput. Ap*.