IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 8, August 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Ensuring Secure Communication by Providing High Security and Data Confidentiality in Wireless Sensor Networks

Mamata[1], Deepak N Biradar[2]

[1]PG Student, Department of Computer Science and Engineering,
[2]Assistant Professor, Department of Computer Science and Engineering,
Lingaraj Appa Engineering College, Bidar, Karnataka State, India.

***Abstract*— A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data item. Such an approach is not suitable for emergent multi-owner- multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named (DiDrip). Next to improve the the security and mutual authentication to each and every node, a trust based model is followed.**

***Keywords*— Distributed data discovery and dissemination, security, wireless sensor networks, efficiency.**

I. INTRODUCTION

Wireless sensor network (WSN) is deployed there is usually a need to update buggy old small programs or parameters stored in the sensor nodes. This can be achieved by the data discovery and dissemination protocol, which facilities a source to inject small programs, commands, queries and configuration parameters to sensor nodes. Note that it is different from the code dissemination protocols which distribute large binaries to reprogram the whole network of sensors. For example, efficiently disseminating a binary file of tens of kilobytes requires a code dissemination protocol. While disseminating several two-byte configuration parameter requires data discovery and dissemination protocol. Considering the sensor nodes could be distributed in a harsh environment, remotely disseminating such small data to the sensor nodes through the wireless channel is a more preferred and practical approach than manual intervention. Motivate by the above observation, this paper as the following main contribution 1 the need of distributed data discovery and dissemination protocol is not completely new, but previous work did not address this need we study the functional requirement of such protocol, and said there design objective. Also we identify the security vulnerabilities in existing data discovery and dissemination protocol.

Sensors have limited memory, computational capability, and limited transmission capacity. The sensors primarily

Pre-programmed to collect the data and forward to the base station through defined communication path. If the information is sensitive, the nodes and communication path must be trust worthy. The sensor network possesses the self-organizing capability if the positions of nodes are not predetermined. Irrespective of the topology, each node must trust the successive node in the path. If any node in the path is suspicious, the decision node must calculate the alternative path. There are varieties of methods to calculate the trust of a successive node. The methods include the reputation-based trust management, event-based trust management, collaborative trust management, and agent-based trust management. In reputation-based trust management, the node stores the number of packets transfer from the node and calculate the success rate of packets transferred from its successive node. In the event-based trust management system, the trust rate is calculated at particular or specific time events or periodically. In collaborative models, the business models are used to calculate the trust similar to product trust management. In agent based trust management systems, an agent node is introduced to store the packet transfer information from a cluster of nodes within communication distance. The agent-based systems relieve the most of the processing time of nodes and the nodes concentrate on transfer of information. Trust-based systems will help to detect the malicious nodes and eliminate them from the communication path.

II. RELATED WORK

As a special sensor network, a wireless body area network (WBAN) provides an economical solution to real-time monitoring and reporting of patients physiological data wireless sensor networks are widely data applicable in monitoring and control of environment parameters. It is sometimes necessary to disseminate data through wireless links after they are deployed in order to adjust configuration parameters of sensors or distribute management commands and queries to sensors. Several approaches have been proposed recently for data discovery and dissemination in WSNs. A data discovery and dissemination protocol, for wireless sensor networks (WSNs) is answerable for updating configuration parameters of, and distributing management instructions to, the sensor nodes. All existing data discovery and dissemination protocols undergo from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data item.

Wireless sensor networks (WSN) are attractive for information discovery in large-scale data rich environments and can add value to mission-critical applications such as

battle-field surveillance, environmental monitoring and emergency response. However, in order to fully exploit these networks for such applications. Data dissemination and discovery is critical for ad-hoc wireless sensor networks. Most existing research depends on location information that is not always obtained easily, efficiently and accurately. We propose the concept of Contour-cast, a location-free data dissemination and discovery approach for largescale wireless sensor networks. Multidimensional WSNs are deployed in complex environments to sense and collect data relating to multiple attributes (multidimensional data). Such networks present unique challenges to data dissemination, data storage and in-network query processing (information discovery). we present simulation results showing the optimal routing structure depends on the frequency of events and query occurrence in the network. It also balances push and pulls operations in large scale networks enabling significant QoS improvements and energy savings. Multicast communication is becoming the basis for a growing number of applications. Therefore, securing multicast communication is a strategic requirement for effective deployment of large scale business multi-party applications. One of the main issues in securing multicast communication is the source authentication service. Sensor networks deployed in hostile areas are subject to node replication attacks, in which an adversary compromises a few sensors, extracts the security keys, and clones them in a large number of replicas, which are introduced into the network to perform insider attacks.

III.PROPOSED SYSTEM

DiDrip consists of four phases, system initialization, user joining, and packet pre-processing and packet verification. For our basic protocol, in system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In user joining phase, a user gets the dissemination privilege through registering to the network owner. In packet pre-processing phase, if a user enters to the network and wants to dissemination some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet. Based on the design objectives, they propose DiDrip. It is the first distributed data discovery and dissemination protocol, which allows network owners and authorized users to disseminate data items into WSNs without relying on the base station. Moreover, our extensive analysis demonstrates that DiDrip satisfies the security requirements of the protocols of its kind. In particular, they apply the provable security technique to formally prove the authenticity and integrity of the disseminated data items in DiDrip.

In this paper, in order to enhance the security and mutual authentication to each and every node, a trust based model is followed. According to this method, the rating of each node is maintained at each node level. The ratings of a node will be done through the ratio of packet forwarded by packets received. The node selection is based on the ratings. The nodes which are having high-rating are considered as trusted one and data packets are routed through them.

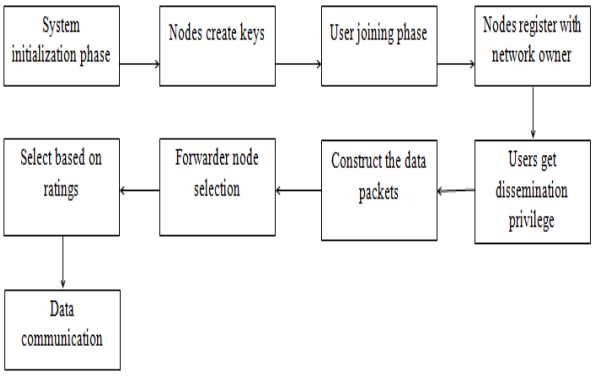

Fig.1 Block diagram of Proposed System

Advantages

- Proposed approach is suitable for multi-owner-multi-user WSNs.
- Identified the security vulnerabilities in data discovery and dissemination when used in WSNs.

IV. IMPLEMENTATION

Modules:

1. WSN creation and routing

In this module, a WSN is created. The sensor nodes and sink in configured and randomly deployed in the network area. The sensor nodes are equipped with energy resource. The sensor nodes are connected with wireless link. The sensor nodes would transmit the data to the Base station nodes. The sensor nodes need to consume the energy to send, receive the data. The communication is enabled in the network between sensor node and base station

2. Implementation of DiDrip protocol

In this module, in system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In user joining phase, a user gets the dissemination privilege through registering to the network owner. In packet pre-processing phase, if a user enters to the network and wants to dissemination some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet.

3. Trust Model

In this work, in order to enhance the security and mutual authentication to each and every node, a trust based model is followed. According to this method, the rating of each node is maintained at each node level. The ratings of a node will

bedone through the ratio of packet forwarded by packets received. The node selection is based on the ratings. The nodes which are having high-rating are considered as trusted one and data packets are routed through them.

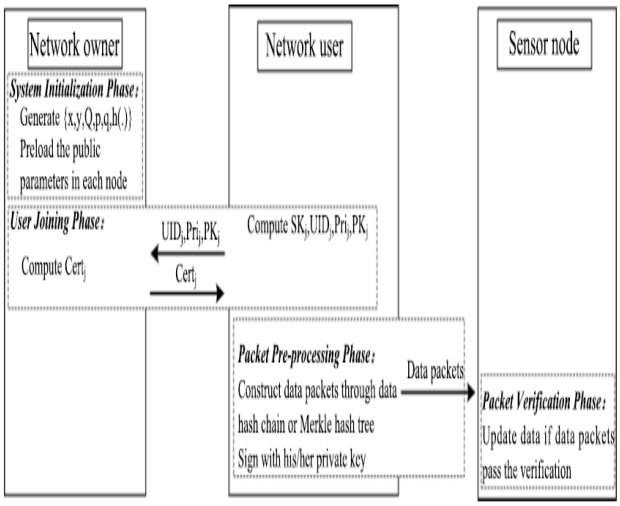

Fig. 2 Information processing flow in DiDrip

DiDrip Protocol mainly includes five phases to disseminate the data between the nodes among the wireless sensor network. Figure 2 shows the information processing flow in DiDrip Secure protocol, which shows the data discovery and dissemination of data from source to destination through the authorized users only, where it contains the following mechanisms.

- Network Owners
- Authorized users
- Sensor nodes

Notation	Description
UID_j	Identity of user U_j
PK_j	Public key of user U_j
SK_j	Private key of U_j
Pri_j	Dissemination privilege for user U_j
$Cert_j$	Certificate of user U_j
$SIG_k(M)$	Signature on message M with key k
h(M)	Hash value of message M
$\|$ or ,	Concatenation of two bit streams

TABLE 1: Notations

A. ***System Initialization Phase***

160 bit Elliptic curve cryptography is set up in this phase. The network owner performs the following steps.

- Choose two big prime numbers p and q each of 160 bits long.
- Select an elliptic curve E over GF(p)
- Select private key x ϵ GF(q).
- Compute the public key y = xQ where Q is the base point of E and is of 320 bits long. y is 160 bits long.
- Load the public parameters {y, Q, p, q} in each node.

B. User Joining Phase

When any user, say Uj wants to join the network and obtain the dissemination privileges, the user joining phase is invoked. The user requests for the certificate from the network owner. The steps are as follows.

- Consider a network user U_j with the identity UID_j which is of two bytes.
- User chooses a private key SK_j ϵ GF(q)
- User computes the public key $PK_j = SK_j.Q$
- User sends a 3-tuple < UID_j, Pri_j, PK_j> to the network owner.
- The network owner generates the certificate and sends back to the user U_j.

$Cert_j$= { UID_j,$PK_j$$Pri_j$, SIG_x{h(UID_j || PK || Pri_j)}}

Since user ID is of two bytes, 65,536 users can be supported. The length of privileges field is of 6 bytes andhence the certificate generated is 88 bytes long.

C. Packet Pre-processing Phase

When a user enters the network and has some information to disseminate over the network, first it has to construct the packet. This is done in packet pre-processing phase. The following steps are performed.

- The user constructs the packet by using Merkle hash tree method.
- Here a tree is constructed taking n data items.
- The data items act as the leaves of the tree.
- At the upper level, internal nodes are constructed by concatenating two child nodes.
- Continue constructing the nodes until the root node is formed. It is labelled as H_{root}.
- Thus obtained tree is the Merkle hash tree with depth $D = \log_n(n)$.
- The user, before dissemination of actual data items,
- Signs the root node $H_{root}$with SK_j.
- Sends an advertisement packet P0
  P0 = {$Cert_j$ || H_{root}|| $SK_j(H_{root})$}
- After sending P0, the user disseminates further packets along with the appropriate internal nodes. In Merkle hash tree method, each packet contains the D hash values.

D. Packet Verification Phase

When any sensor node receives the disseminated data, it has to first verify whether it is from authorized user, whether that sensor node ID is included in the node identity set of Pri_j and

whether the packet maintains data integrity. The following steps are performed.

- If the packet received is advertisement packet
  P0 = {Cert$_j$ || H$_{root}$|| SK$_j$(H$_{root}$)}, check for the privileges.
- If the result is positive, then check for the authenticity if certificate by using the public key, y of the network owner.
- If certificate is valid, check for the validity of signature.
- If the result is positive then store <UID$_j$, root>, otherwise discard the packet.
- If the packet received is a data packet other than P0, the sensor node checks for the authenticity and integrity.
- For positive result, it checks for the freshness of the data. If the packet received is a newer version, then it updates its data.

V. RESULTS

After implementing the proposed system on NS2 platform, the results obtained are as follows:

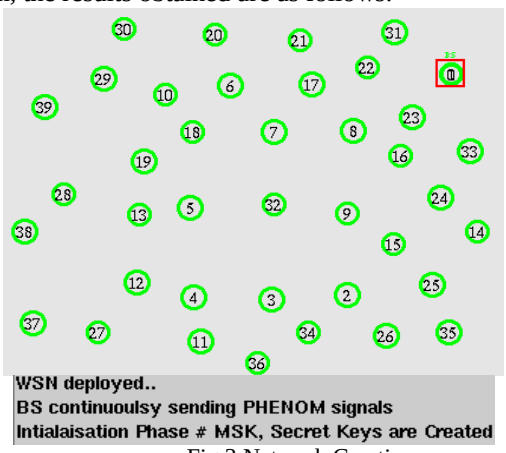

Fig.3 Network Creation

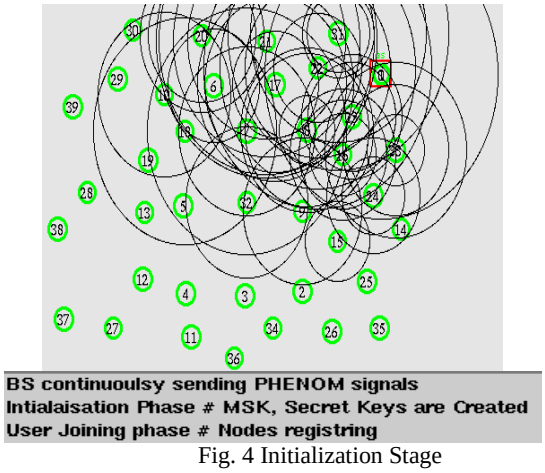

Fig. 4 Initialization Stage

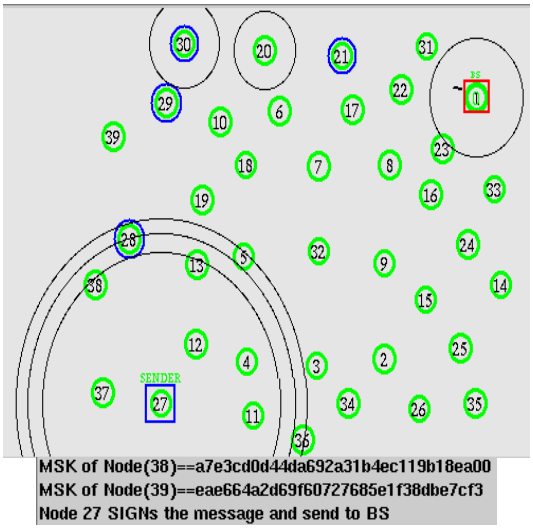

Fig. 5 Transmission Stage

Figure 3 shows the network creation stage, where we can able to see the topology formed, and nodes are configured. The base station is visible as node 0, which is sending the phenom signals continuously. And in this stage, secret keys are created for each node in the network.

Figure 4 shows the initialization phase, the nodes present within the network receives the secret key,usig which the nodes communicates with each other within the network.

Figure 6 shows throughput comparison graph, where it shows the proposed system is better as compared to the existing system.

Fig. 6 Throughput comparison graph

The figure 7 shows the energy comparison graph. The graph shows that the proposed system's performance is better i.e. the proposed system utilized less energy as compared to the existing sytem.

Fig. 7 Energy consumption graph

VI. CONCLUSIONS

Considering such a problem with wireless sensor network in accordance with the security is more complex and challenging in nature and the security vulnerabilities in data discovery and dissemination when used in WSNs. An energy efficient new AP algorithm has been proposed. Thus we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols and AP algorithm and the system will maintain the integrity of the data also ensure the performance of the system.

Here we can conclude that the proposed system will provide the high security. Then by applying energy efficient new algorithm we can encrypt and decrypt the message for the security purpose. We proposed a new symmetric key AP algorithm based on shuffling, substitution and shifting to depict a security scheme for WSN which is energy efficient as well as difficult to crack. In this research we will not only going to detect the malicious node from the network, but we will also remove the attacker node from the network, which will make the system much more secure and reliable. This will provide us a high security to the wireless sensor network by detecting and removing the attacker from the network. The analysis was performed in network simulator (NS2).

REFERENCES

[1] Sneha Ghormare, Vaishali Sahare, " A Survey on Data Confidentiality for Providing High Security in Wireless Sensor network",International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume-5, Issue-1, , pp. 249-252, January – 2015.

[2] D. He, S. Chan, Mohsen, Guizani, H. Yang, "Secure and distributed data discovery and dissemination in Wireless Sensor Network", IEEE Trans. Parallel and distributed system, 2014

[3] Archana Tayal, Prachi , "Energy Efficient New Symmetric Key Algorithm (AP) for WSN", Research Notes in Information Science (RNIS) Volume13, May 2013 doi:10.4156/rnis.vol13.35.

[4] D. He, C. Chen, S. Chan and J. Bu, "DiCode: DoS resistant and distributed code dissemination in wireless sensor networks", IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012.

[5] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638-4646, Sept.2013.

[6] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Department of Computer Science Wayne State University, 2006 Auerbach Publications, CRC Press.

[7] Ritu Sharma, Yogesh Chaba Yudhvir Singh, "Analysis of Security Protocols in Wireless Sensor Network", Int. J. Advanced Networking and Applications 707 Volume: 02, Issue: 03, Pages: 707-713 (2010).

[8] R.C. Shah, S.Roy, S. Jain, W.Brunette, "Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks," in IEEE International Workshop on Sensor Network Protocols and Aplications, 2003.

[9] J.Hill, R.Szewezyk, A.Woo, S.Hollar, D.Culler and K.Pister, "System Architecture Directions For Networked Sensors," ASPLOS, 2000.

[10] E.Hamida, G.Chelius, "Strategies for Data Dissemination to Mobile Sinks in Wireless Sensor Networks," IEEE Wireless Communication, vol.15, no.6, pp.31-37, Dec. 2008