International Journal of Computer Applications (0975 8887)
Volume 82 - No. 11, November 2013

Multicast Authentication Framework for Hierarchical Networks using Chinese Remainder Theorem

Priyanka Sadananda
School of Electronics Engineering
Vellore Institute of Technology
Vellore-632014, India

Wassim Trojet
Telecommunication Network Lab
IRSEEM
Rouen, France

Joseph Mouzna
Telecommunication Network Lab
IRSEEM
Rouen, France

ABSTRACT

For dense deployment of sensor nodes required in many environmental monitoring applications, an hierarchical network organization offers distinct advantages over flat networks. Broadcast and multicast, being the principle modes of communication in these networks, require confidentiality and authentication to prevent adversaries from broadcasting false messages. In this work, an authentication framework for hierarchical networks is proposed that permits authenticated and secure broadcast from base station as well as middle tier nodes using Chinese remainder theorem(CRT). The proposed protocol uses different prime numbers in each cluster to generate unique CRT solutions for authenticating multicast messages by cluster head. We shall describe our strategy for the distribution of prime numbers to establish initial trust in the network. Further, we shall prove that multicast authentication using CRT is ideal for clustered network organization in terms of energy efficiency and tolerance to attacks.

Keywords:

Wireless Sensor Networks, Multicast, Authentication, Chinese Remainder Theorem

1. INTRODUCTION

Recent works have proposed the deployment of wireless sensor networks for safety critical applications such as fire detection systems[1], structural health monitoring[2] and activity monitoring/target tracking in military environments[3](eg. Border surveillance). The wireless nature of communications and the deployment of nodes in hostile environment makes the system vulnerable to eavesdropping and physical compromise by attackers. Therefore, security must be added to ensure confidentiality and integrity of sensor messages. Broadcast is the main mode of communication in wireless sensor networks. Several messages like queries, routing messages, alerts and network programs need to be broadcasted to the target nodes in a secure and reliable manner. The limited memory and energy of the sensor nodes also place stringent requirements on the security of the broadcast protocol. Therefore, the protocol used for broadcast must be designed exclusively for the network at hand by taking into account, the nature of the WSN application and network architecture in order to save energy and prolong network lifetime.

The critical applications described previously generally require the installation of a large number of nodes over the geographical area to be surveilled. In such large scale sensor networks, Clustering offers distinct privileges over a flat organized sensor network in terms of energy, bandwidth saving and improved scalability. It also provides distributed control over the network thereby simplifying routing and data aggregation. The advantages of introducing hierarchy in network architecture had been extensively researched and widely proven[4][5][6].

While broadcast security in flat sensor networks has been frequently addressed in previous works, very few works focus on broadcast authentication in clustered networks. The hierarchical organization of these networks implies that the cluster head nodes have certain level of authority and control over the common nodes. It is therefore necessary and desirable to authenticate multicast messages within clusters. This would significantly save bandwidth as well as minimize the load on the base station.

Apart from authentication, it is also necessary to guarantee confidentiality of the message within the cluster. For instance, if network programs need to be broadcasted in a military surveillance network, it may be required for only nodes in a particular cluster to be reprogrammed. It is preferred that other nodes in different clusters need not know the contents of this broadcast message since any other cluster might contain compromised nodes.

The approaches for broadcast authentication fall in two main categories: algorithms using symmetric-key cryptography and those that use public key cryptography. Symmetric key techniques rely on a message authentication code(MAC) calculated over the message using the shared key between the nodes to provide authentication. Public key techniques on the other hand use 2 keys: public and private key to generate a digital signature for the message. Due to the difficulties in applying public key cryptography in resource constrained WSN nodes, this work focuses only on symmetric key approaches to secure multicast in clustered networks. One possible solution is to use a shared key among the cluster nodes. This approach, however is vulnerable to node impersonation attack in case an attacker obtains the shared key from a compromised node. Another solution is to use uTESLA[7] in clustered networks, where the base station generates the MAC for the cluster head whenever it wishes to multicast a message. Since the base station is responsible for disclosure of keys, this technique would be robust against node compromise but it results in authentication delay. In most of the applications, broadcast messages are sudden non periodic alerts and therefore cannot tolerate any delay.

To solve these issues, a multicast authentication method is proposed

that is tailored to clustered networks based on Chinese remainder theorem. The proposed solution uses Chinese remainder theorem to authenticate the message as well as provide a secure lock over the message so that it can be accessed only by the valid members of the cluster group. Through this paper, we shall show that the proposed solution is computationally inexpensive, allows immediate authentication and guarantees confidentiality of multicast communication within clusters. The remainder of the paper can be organized as follows. Section II summarizes a number of prior approaches proposed to tackle the problem of broadcast authentication. Section III provides the problem statement and states the assumptions used in the proposed protocol. Section IV briefly describes the background theory required for this work. Section V provides a comprehensive description of the framework which is followed by simulation results in Section VI and a discussion of obtained results in Section VII.

2. PREVIOUS WORK

A number of works have explored the problem of broadcast authentication and have proposed both symmetric and asymmetric cryptographic approaches to provide security. For the purpose of comparison, only approaches that use symmetric cryptography primitives are mentioned here. In [7], Adrian Perrig et al proposed a suite of security protocols called SPINS for providing security to sensor networks. They proposed a protocol uTesla that used delayed key disclosure and time synchronization between base station and nodes to provide broadcast authentication. This technique suffers the following disadvantages. Firstly, the buffering of messages at the receivers till the key disclosure period makes the system vulnerable to DoS attack. In uTesla, the receiver nodes have to buffer the message till they receive the corresponding key from the base station. During this period, an attacker could flood the receiver with false messages thereby causing it to reject authentic base station messages due to unavailability of buffer space. Secondly, the number of authentications is limited by the length of the hash key chain generated at the base station. To solve the first problem, Perrig et al proposed buffering of messages at the sender in [8] and a number of works[9][10] proposed weak authenticators to pre-filter the message before the keys are received. In [11], Liu et al attempted to solve the second problem by using multiple levels of hash key chains to prolong the lifetime of uTesla.

An interesting approach to authentication of Base station broadcasts has been presented in [12]. The authors use Chinese remainder theorem to associate together the MAC of the message and the key. This CRT solution is broadcasted to every node. Valid nodes of the network can authenticate the message as they contain the prime numbers used to generate the CRT solution. This approach has been enhanced in [13] where the hash of the next key is also incorporated in the CRT solution. This allows independent keys to be used that permit infinite number of authentications. The simplicity of this approach and the ability to meet the basic requirements of broadcast authentication has encouraged us to apply this technique for cluster head authentication in hierarchical WSN.

A number of protocols were proposed that specifically addressed the problem of security in clustered sensor networks. In [14], the authors describe a key management protocol that uses four keys: individual key, group key, cluster key and pair wise key to satisfy different security requirements. Another work that targets hierarchical networks with an arbitrary number of levels is LHA-SP[15].Oliveira et al describe a key distribution strategy to setup shared keys between nodes at different levels. It addresses broadcast authentication by setting up a shared key between the cluster head and groups of its child nodes. Work [16] adds security on top of the LEACH clustering protocol and uses uTesla to authenticate broadcast messages with the MAC for the message broadcasted by the cluster head being generated by the base station. In [17], Bohge et al propose tesla certificate, a purely symmetric alternative to public key certificates that can be used for authentication of broadcasts. In [18], the authors address the problem of cluster head broadcast by proposing a distributed scheme based on uTesla. The authors propose a trust establishment scheme that allows the cluster head to authenticate messages using its own hash chain. This distributed scheme is compared with a centralised scheme in which the base station generates the MAC for the message broadcasted by cluster head.

To evaluate the proposed protocol, we have chosen to compare it with centralised uTesla and Distributed uTesla as described in [18]. Both uTesla based schemes are described as follows.

2.1 Centralised uTesla

In this case, whenever the cluster head wishes to broadcast a message, it sends to the base station,the encrypted message and MAC created by using its pairwise key with the base station. The base station verifies the message and generates the MAC for the message using its current key which it will disclose during the following time interval. It sends this message to the cluster head which broadcasts it to all its cluster nodes along with the message. After the key disclosure delay, the base station broadcasts the key to the entire network thereby allowing the cluster nodes to verify the MAC. The major disadvantage of this method is that network wide broadcasts are required whenever the cluster head needs to broadcast a message. To overcome this problem, the authors propose distributed uTesla.

2.2 Distributed uTesla

In the distributed scheme, each cluster head node has a hash chain of keys: K_{ch1},K_{ch2},K_{ch3}.....K_{chN}. The base station also generates a hash chain of keys:K_{b1},K_{b2},K_{b3}.....K_{bN} and K_{bN} is preloaded into all the nodes in the network. Each cluster node is also provided with an authentication code $MAC(K_{chN}, K_{b(N-1)})$. After deployment, the cluster head broadcasts the following message:

$$< K_{chN}, MAC(K_{chN}, K_{b(N-1)}) >$$

The cluster nodes buffer this message until the disclosure of the key, $K_{b(N-1)}$ by the base station. The nodes can now authenticate K_{chN} and save it as the key chain commitment for the cluster head so that future messages from the cluster head can be authenticated. Although this technique reduces the base station involvement, it still presents the problem of authentication delay. However, this scheme provides an ideal solution for the establishment of trust between the the cluster head and cluster nodes.

3. PROBLEM STATEMENT AND ASSUMPTIONS

The main goal of this work is to propose a multicast protocol for clustered networks that is robust to common attacks like Denial of Service(DoS), eavesdropping, modification, replay and node impersonation and is energy efficient and computationally simple for resource constrained sensor nodes. The expected outcomes of this work are enumerated as follows:

(1) Describe a protocol that guarantees confidentiality and authentication for multicast messages by cluster head nodes.

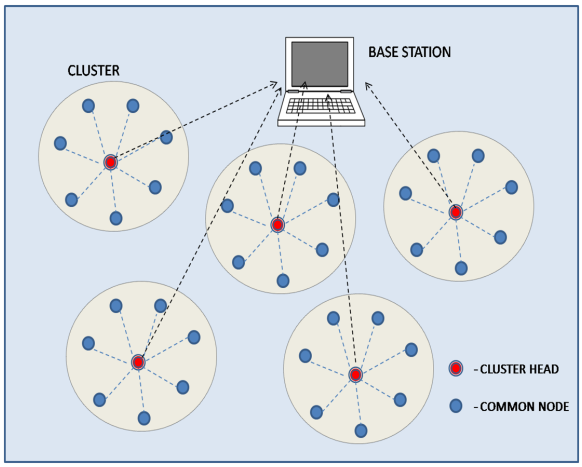

Fig. 1. Typical clustered network

(2) Provide a solution for the initial establishment of trust in the network.

(3) Analyse the protocol in terms of energy efficiency and resilience to common attacks against broadcast security.

3.1 Assumptions

A large scale hierarchical wireless sensor network is considered with hundreds of nodes. Only 2 levels of hierarchy are assumed. Therefore, the network consists of a central base station, cluster head nodes and normal cluster nodes. The cluster head nodes may be fixed before deployment or decided later based on some clustering algorithm. The actual algorithm used for clustering as well as the security of the clustering technique itself is out of scope of this paper. It is assumed that once clusters are formed, re-clustering takes place only after a long time interval. This provides sufficient time for the clusters to be formed and for the proposed setup protocol to take place.

The base station is assumed to be a node with higher computational capability and with no constraint of energy. The cluster nodes are assumed to have limited memory and energy. The network architecture that is assumed in this work is shown in figure 1.

It is also assumed that there exists a finite time interval between the time at which the nodes are deployed and when an attacker is able to physically compromise a node. It is during this finite time interval that keys are distributed and trust relationships are established in the network.

During and after this time interval, it is possible for an attacker to eavesdrop on the messages as well as broadcast his own messages into the network. We do not address replay attack and believe that it can be countered by including a timestamp along with the message to be encrypted.

The principle communication type that this work focuses on is intracluster broadcast messages,ie broadcast message from the cluster head to its child nodes. Apart from this, it also addresses base station broadcasts to the entire network. The security of unicast communications is out of scope of this paper. For simulation purposes, pairwise keys between nodes have been used to provide unicast security.

4. BACKGROUND THEORY

First, we will describe the broadcast protocol based on chinese remainder theorem as used in [13] and follow it by a detailed explanation of chinese remainder theorem and finally describe the proposed protocol that adapts this technique to clustered sensor networks.

4.1 Broadcast Authentication using CRT

In this method, it is assumed that all nodes in the network are preloaded with 3 relatively prime numbers. The Base station generates a set of independent keys(one for each message) which it will use to generate the MAC for broadcast messages. The hash of the first key that the base station wishes to use is also preloaded into all the nodes. Whenever the Base station wishes to broadcast a message, it first generates the MAC of the message using its current key. Then, it solves 3 congruent equations involving the MAC of the message, the current key, the hash of the next key and the three preloaded prime numbers. This unique CRT solution is broadcasted to all nodes along with the message. Since the nodes contain the prime numbers, they can extract the MAC, current key and hash of next key by using simple modulo operations. Using the current key and message, they can generate a MAC and compare with the broadcasted MAC. They can verify the sender by hashing the key and comparing with the preloaded value. The hash of the next key can be stored for authenticating the key in the next message.

4.2 Generalised Chinese Remainder Theorem

Let $p_1, p_2, p_3 ... p_N$ be a set of pairwise relatively prime numbers. Let $r_1, r_2, r_3 ..... r_N$ be a set of positive integers such that $r_i < p_i \forall i \in [1, N]$. Let X be the solution of a set of congruent equations(equation (1)) where $\equiv$ is used to represent congruence.

$$\begin{aligned} X &\equiv r_1 \pmod{p_1} \\ X &\equiv r_2 \pmod{p_2} \\ X &\equiv r_3 \pmod{p_3} \\ &\vdots \quad\quad \vdots \\ X &\equiv r_N \pmod{p_N} \end{aligned} \tag{1}$$

Chinese remainder theorem states that a unique solution for X exists and lies between $[1, N-1]$. This unique solution is given by equation(2).

$$X = \sum_{i=1}^{N} q_i * r_i * y_i \pmod{P} \tag{2}$$

where,

$$P = p_1 * p_2 * p_3 ..... * p_N \tag{3}$$

$$q_i = \frac{P}{p_i} \tag{4}$$

and,

$$q_i * y_i \equiv 1 \pmod{p_i} \tag{5}$$

y_i is determined by using extended euclid's theorem.

5. PROPOSED PROTOCOL

The proposed protocol uses CRT to provide multicast authentication for cluster heads in the same manner as described in Sec-

tion 3.A. Further, it proposes a setup strategy to distribute different prime numbers to each cluster and thereby adapts this protocol to clustered network . The proposed protocol is outlined in the following steps and summarized in Figure 2. The setup phase of this protocol can be divided into 3 stages: initialization, generation of prime numbers and setup of cluster. On completion of these 3 stages, future authentication of multicast messages within clusters can be easily achieved.

5.1 Initialization

(1) Prior to the deployment of nodes in the network, 4 prime numbers: n_1, n_2, n_3, n_4 are pre-loaded into all the nodes.

(2) The base station generates a set of independent keys:K_1, K_2, K_3..... and stores the hash of the first key $(H(K_1))$ in all the nodes.

(3) After deployment, clustering takes place. Once clusters are formed, each cluster head generate a set of keys and computes the hash of the first key(K_{ch1}). He then encrypts it and finds the MAC for it by using his pairwise key shared with the base station(K_{CBi}). The message which is now of the form(equation 6) is sent to the base station.

$$< encrypt(H(K_{ch1}), K_{CBi}), MAC(H(K_{ch1}), K_{CBi}) > \quad (6)$$

5.2 Generation of prime numbers

(1) The base station receives the message, decrypts it and verifies it by using the MAC. It now generates 3 random prime numbers: $p1, p2, p3$ for the corresponding cluster.

(2) The base station concatenates the prime numbers to form

$$p = (p_1 \parallel p_2 \parallel p_3)$$

. It encrypts 'p' by using its current key and calculates the MAC for 'p' using the same key.

(3) Then, it computes MAC for the received $H(K_{ch1})$ using its current key and also finds the hash of the next key(K_2) that it plans to use for future broadcast.

(4) The CRT solution is calculated from the following congruent equations.

$$\begin{aligned} U &\equiv MAC(p, K_1) && (\text{mod } n_1) \\ U &\equiv MAC(H(K_{ch1}), K_1) && (\text{mod } n_2) \\ U &\equiv K_1 && (\text{mod } n_3) \\ U &\equiv H(K_2) && (\text{mod } n_4) \end{aligned} \quad (7)$$

(5) The message sent by the base station will now be of the form as shown in equation 3. Base station will send this message to the cluster head.

$$< encrypted(p, K_1), U > \quad (8)$$

(6) The cluster head further broadcasts this message to its members within the cluster radius.

5.3 cluster setup

(1) The cluster nodes accept the broadcast message from their respective cluster heads. Since they contain n_1, n_2, n_3, n_4, they can obtain the MAC data and key from U using simple modulo operations as shown in equation (2).

$$\begin{aligned} MAC(p, K_1) &= U && (\text{mod } n_1) \\ MAC(H(K_{ch1}), K_1) &= U && (\text{mod } n_2) \\ K_1 &= U && (\text{mod } n_3) \\ H(K_2) &= U && (\text{mod } n_4) \end{aligned} \quad (9)$$

(2) Using K1, the nodes can decrypt the message and obtain the 3 prime numbers p_1, p_2 and p_3.

(3) Now, they calculate MAC of $p_1||p_2||p_3$ and compare it with the MAC from equation (2) to authenticate the message.

(4) The nodes hash K_1 and compare with the preloaded H(K_1) to ensure that the sender is an authentic one.

(5) if any of the above 2 tests fail, the nodes will reject this message. Otherwise, the nodes will store $p_1, p_2, p_3, K_1, H(K_2)$ for future authentication.

(6) MAC(H(K_{ch1}), K_1) and K_1 can be stored by the cluster heads to authenticate the first message sent by the cluster head. This way, the nodes can guarantee the authenticity of the source when the source is the cluster head.

5.4 Future Broadcast

Any future broadcast is done only using the corresponding prime numbers of the cluster: p_1, p_2 and p_3. The cluster head generates the message, encrypts it if necessary and calculates the CRT solution as shown in equation 10.

$$\begin{aligned} U &\equiv MAC(message, K_{current}) && (\text{mod } p_1) \\ U &\equiv K_{current} && (\text{mod } p_2) \\ U &\equiv H(K_{next}) && (\text{mod } p_3) \end{aligned} \quad (10)$$

The broadcast message for the cluster is of the form shown in equation 11.

$$< encrypt(message, K_{current}), U > \quad (11)$$

When a new cluster sends a request to the base station, it receives a unique set of prime numbers that is different from that of other clusters. Since different nodes use different prime numbers, confidentiality is achieved for intra-cluster broadcasts. Intercluster broadcast can be carried out through cluster heads. For global broadcasts by the base station, the global preloaded prime numbers: n_1, n_2, n_3 can be used.

6. SIMULATION

6.1 Simulation Setup

The proposed algorithm network was simulated using NS-2.35, a discrete event simulator and Mannasim[19]. The simulated network consists of a central base station, cluster head nodes and ordinary sensor nodes. The algorithm used for clustering is not discussed in this paper. In all the simulation scenarios, the inter node spacing is fixed at 40m with the nodes arranged in a rectangular grid topology. The cluster size is fixed to 25. The simulation parameters are outlined in Table 1 and the simulated network is depicted in figure 3.

Encryption of messages is carried out using AES-128 algorithm and the hash function used is SHA-1. OpenSSL cryptographic library was used for the underlying cryptographic primitives. For the CRT algorithm, 8 byte prime numbers were used to generate the solution. All simulations were carried out on a core 2 duo processor operating at 2.66GHz and 4GB RAM.

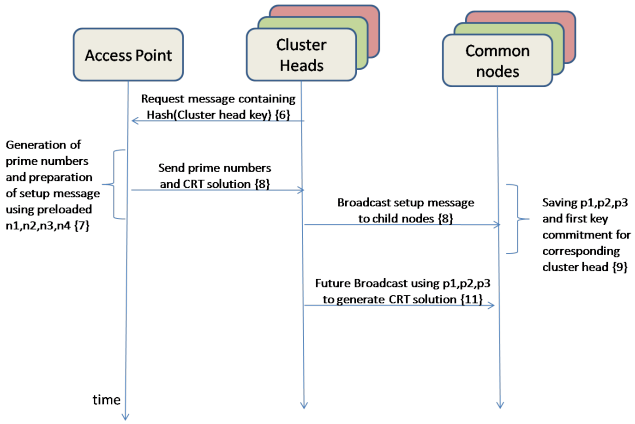

Fig. 2. Sequence diagram showing message exchange between sensor nodes. The numbers within braces indicate the corresponding equations

Table 1. Simulation Parameters

PARAMETERS	VALUE
Number of access points	1
Number of cluster heads	4
Number of common nodes	96
Cluster size	25
Transmission range of nodes	100m
MAC protocol	IEEE 802.11
Routing Protocol	AODV
Propagation model	Two ray ground
Simulation time	100s
Interval between broadcasts	1s
Key disclosure delay for uTesla	0.6s
Scenario size	400m X 400m
TxPower of cluster head	1 W
RxPower of cluster head	0.3 W

The protocol is evaluated by comparing it with uTesla adapted to a clustered network. Both centralised and distributed schemes described in Section II were simulated using NS2. In addition, the two protocols were modified by adding encryption to the data using the same keys that are used to generate the authentication codes. In the simulation, the duration of each key interval and the key disclosure delay were fixed as 0.5s and 0.6s respectively for the uTesla protocol.
The scenario considered for all three cases is as follows: Each network carries out its initialization phase. After the establishment of initial trust in the network, the cluster head broadcasts a message to its child nodes every 1s for a total duration of 100s.

6.2 Simulation Results

First, the efficiency of the setup phase in the proposed framework is analyzed by analyzing the time required for a cluster to complete the setup phase. The proposed multicast protocol is then compared with uTesla in an hierarchical network architecture in terms of energy efficiency and authentication delay. With regard to uTesla, both centralized and distributed schemes are implemented for comparison.

6.2.1 Setup time. In order to determine the time required for the setup of the clusters, the time required to setup one cluster in the network is calculated as a function of the network size. After the clustering has taken place, the cluster head sends a request to base station, receives the prime numbers and multicasts it to its child nodes. This completes the setup phase. The setup time is therefore a combination of transmission times, propagation delay and the time required for the base station to generate the CRT setup message(Equation 8) for the cluster. The setup time provides a measure of the efficiency of the initial setup protocol and determines if the proposed protocol is scalable for large networks. These results are presented in Figure 4. The network size is increased proportionately by maintaining the inter-node as 40m, cluster size as 25 and fixing the base station at the center of the network. The time required at the base station to generate prime numbers and calculate the CRT value to be broadcasted has been determined to be 0.01s. For a network size of 900 nodes, the time required to setup a cluster is 6.21s . This includes the time required to route messages to and from the base station as will the time required to generate the CRT solution. Shorter setup times can be obtained by increasing the range of the base station. It is reasonable to assume that during this short interval, no attacker tries to compromise a node. We believe that this setup delay is tolerable for such a large scale network.

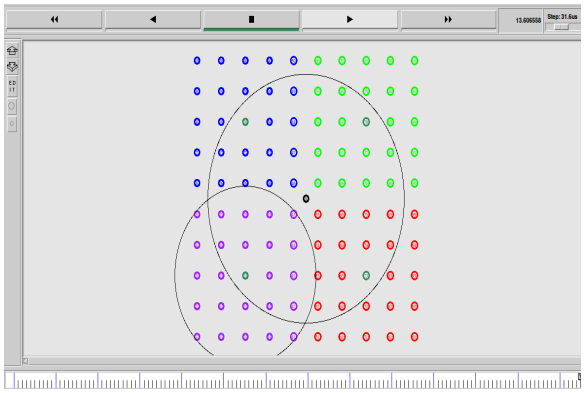

Fig. 3. Simulated network topology. Different colors are used to represent clusters setup with different prime numbers

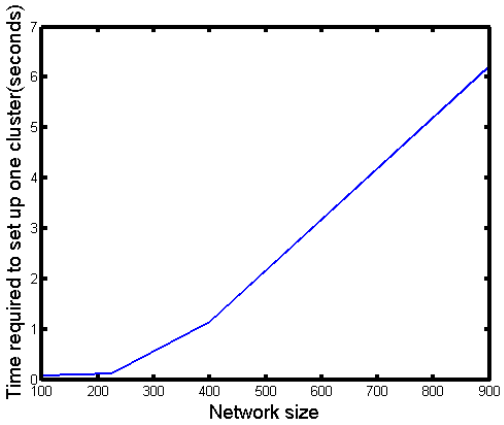

Fig. 4. SIMULATION RESULTS: time required to setup all the clusters Vs network size. The size of a cluster is assumed to be 25

6.2.2 Energy Consumption. The most important criteria that affects the choice of broadcast protocol in sensor networks is energy efficiency. Since sensor nodes have limited energy resources, min-

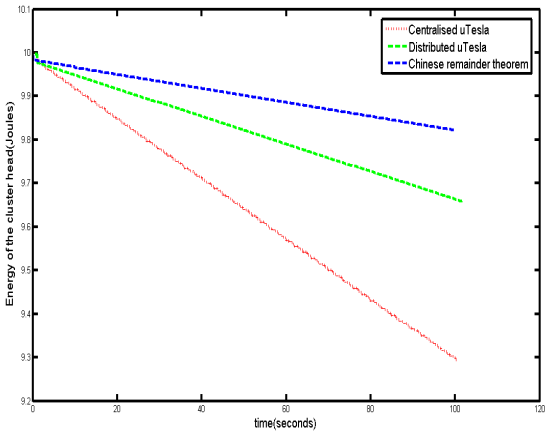

Fig. 5. SIMULATION RESULT: Comparision of energy consumptions of proposed method and uTesla

imization of energy consumption must be the main consideration while designing the multicast protocol. Figure 5 compares the energy consumption of the cluster head nodes with time in both CRT based cluster multicast as well as uTesla based multicast protocols. From figure 4, it is clear that the energy of cluster head in uTesla degrades much faster than in CRT based multicast protocol. The energy consumption of the cluster head nodes at the end of 100 broadcasts in CRT, centralised uTesla and distributed uTesla are 0.18J, 0.708J and 0.34J respectively. In centralised uTesla based multicast, at the end of 100 broadcasts by the cluster head, its energy is lower than the proposed protocol by 0.528J. This can be explained by the higher number of transmissions in centralised uTesla due to the involvement of the base station. In centralised uTesla, the cluster head needs to make 3 transmissions: the initial request to the Base station, broadcast of MAC to child nodes and broadcast of key to child nodes. Although the overhead is more in CRT based multicast, only a single transmission is required by the cluster head node to send a message to its cluster nodes. In distributed uTesla,the energy is lower than CRT based broadcast by 0.16J. In this protocol, once trust has been established in the cluster, the cluster head can directly broadcast to the cluster nodes without the involvement of the base station. Therefore, it has lower energy consumption than centralised uTesla. However, it still needs to broadcast 2 messages: the encrypted message along with authentication code and the authentication key that is disclosed after the predetermined time interval.

6.2.3 Authentication Delay. The delay in authentication of the message broadcasted by the cluster head node Vs its distance from the base station is shown in Figure 6 for all three protocols. Centralised uTesla based multicast protocol presents a delay of 0.6s additional to the transmission delay due to the delayed disclosure of keys by the base station. Further, in centralised uTesla, the delay depends on the propagation delay that is dependent on the distance between the base station and cluster head since the base station is responsible for generating the MAC of the message to be broadcasted by the cluster head. In the CRT based protocol, on the other hand, the multicast authentication delay is independent of the distance from the base station as the cluster head can generate its own MAC for the broadcast message. Therefore, the total authentication delay is a combination of transmission and propagation delays

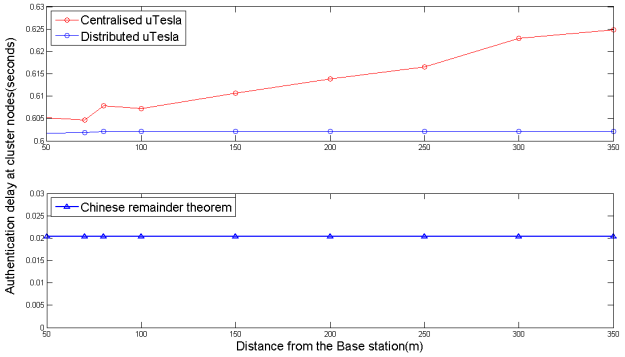

Fig. 6. SIMULATION RESULT: Comparision of multicast authentication delay in uTesla and proposed method

from cluster head to its child nodes. In distributed uTesla, the base station is not required to authenticate the broadcast messages of the cluster head. The only delay involved in the distributed scheme is the key disclosure delay and the propagation delay from the cluster head to its nodes.
A detailed analysis of the proposed protocol with regard to its advantages and resilience to attacks is presented in the next section.

7. DISCUSSION

The proposed method seeks to solve the problem of multicast authentication in clusters and does so by using Chinese remainder theorem with different prime numbers allotted to each cluster. The prime numbers not only help in generating a unique CRT solution that form a signature for the message, but it also helps in securing the message against other clusters. Even if an attacker has compromised one cluster, He cannot read a secret message broadcast in a different cluster. Since the key used to encrypt each multicast message is incorporated into the CRT solution, it is possible only for valid member nodes to obtain the key from the CRT solution and decrypt the message.
In most networks, the cluster nodes are decided after the deployment. Even in this situation, our setup strategy helps in distribution of prime numbers as well as in distributing the cluster head's first key commitment. Even new cluster heads can be setup using the same setup algorithm as long as it is preloaded with the global prime numbers and shares a unique key with the Base station. In case a node is moved or displaced, it can request the base station for the corresponding cluster keys.
Since Chinese remainder theorem is underlying algorithm for broadcast, it permits independent keys to be used thereby allowing infinite rounds of authenticated broadcast. The setup time is also small and therefore the proposed method is scalable for very large sensor networks.
Compared to uTesla in hierarchical networks (Centralised and distributed schemes), the CRT based multicast protocol is energy efficient and does not present large authentication delay. Also the CRT algorithm is computationally simple and easy to implement on sensor node platforms. Although it does add more communication overhead when compared to uTesla, the reduced number of transmissions eventually lowers the energy consumption in CRT based multicast. The overhead in uTesla comprises of the MAC of the message while the overhead in CRT based multicast is the solved

CRT value. The length of this CRT value depends on the length of the generated prime numbers. If p_1, p_2, p_3 are the prime numbers used in CRT, then the value of the unique solution is always lower than $p_1 * p_2 * p_3$.

With regard to attacks, the Chinese remainder theorem based broadcast guarantees immediate authentication thereby tackling the DoS(Denial of Service) problem faced by uTesla. Unlike uTesla, this method does not require the network to be time synchronized. It is therefore, ideal for the broadcast of non periodic messages.

Now, we shall address the issue of node compromise. If a node other than the cluster head is physically compromised, it cannot impersonate the cluster head as it is not aware of the next key that will be used by the cluster head. However, if the cluster head is compromised, it can easily broadcast false updates to its cluster nodes. Therefore, the proposed protocol is unable to tackle cluster head compromise. This problem is not present in uTesla protocol since the Base station is responsible for all the authentication keys. However, the clustered architecture of the network provides a solution to mitigate this issue. If a cluster node begins to broadcast bogus messages that results in faulty cluster node behavior, it can be easily detected by the base station. The base station is aware of all cluster head ids as well as their prime numbers. It must simply listen to the broadcast messages, identify the malicious cluster head node and revoke it. It can later choose a different cluster head and re-distribute the prime numbers.

8. CONCLUSION

In this paper, a possible approach has been discussed to provide confidentiality and authentication to multicast messages within clusters based on Chinese remainder theorem. We provide a solution for the distribution of prime numbers to clusters and establishment of initial trust. Simulation results show that the proposed method has lower energy consumption and authentication delay than uTesla when adapted to a hierarchical network. Moreover, the Chinese remainder theorem provides a secure lock over the message so that it can be read only by the valid members of the cluster who possess the prime numbers.

9. REFERENCES

[1] M.Bri D.Sendra S Lloret, J.Garcia. A wireless sensor network deployment for rural and forest fire detection and verification. *Sensors*, 9:8722–8747, 2009.

[2] Steven D. Glaser. Some real-world applications of wireless sensor nodes. In *In SPIE Symposium on Smart Structures Materials / NDE 2004*, pages 344–355. SPIE Press, 2004.

[3] Jun He, Mahmoud Fallahi, Robert A. Norwood, and Nasser Peyghambarian. Smart border: ad-hoc wireless sensor networks for border surveillance. pages 80190Z–80190Z–7, 2011.

[4] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, pages 10 pp. vol.2–, 2000.

[5] O. Younis and Sonia Fahmy. Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *Mobile Computing, IEEE Transactions on*, 3(4):366–379, 2004.

[6] Mao Ye, Chengfa Li, Guihai Chen, Jie Wu, and Mao Ye Et. Al. Eecs: An energy efficient clustering scheme in wireless sensor networks. In *In: Proc. of the IEEE Intl Performance Computing and Communications Conf*, pages 535–540. IEEE Press, 2005.

[7] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. Spins: security protocols for sensor networks. *Wirel. Netw.*

[8] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and secure source authentication for multicast. In *In Network and Distributed System Security Symposium, NDSS 01*, pages 35–46, 2001.

[9] Hu Xiangdong and Feng Rui. Message broadcast authentication in utesla based on double filtering mechanism. In *Internet Technology and Applications (iTAP), 2011 International Conference on*, pages 1–4, 2011.

[10] Peng Ning, An Liu, and Wenliang Du. Mitigating dos attacks against broadcast authentication in wireless sensor networks. *ACM Trans. Sen. Netw.*

[11] Donggang Liu and Peng Ning. Multi-level uTESLA: Broadcast authentication for distributed sensor networks. *ACM Transactions in Embedded Computing Systems (TECS)*, 3(4):800–836, November 2004.

[12] Jianmin Zhang, Wenqi Yu, and Xiande Liu. Crtba: Chinese remainder theorem-based broadcast authentication in wireless sensor networks. In *Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on*, pages 1–4, 2009.

[13] Sonali S. Mhatre, Vandana B. Salve, and Sonali J. Mane. Article: Enhanced chinese remainder theorem based broadcast authentication in wireless networks. *International Journal of Computer Applications*, 50(15):10–14, July 2012. Published by Foundation of Computer Science, New York, USA.

[14] Sencun Zhu. Leap: Efficient security mechanisms for large-scale distributed sensor networks. pages 62–72. ACM Press, 2003.

[15] L.B. Oliveira, Hao Cho Wang, and A. A F Loureiro. Lha-sp: secure protocols for hierarchical wireless sensor networks. In *Integrated Network Management, 2005. IM 2005. 2005 9th IFIP/IEEE International Symposium on*, pages 31–44, 2005.

[16] Leonardo B. Oliveira, Adrian Ferreira, Marco A. Vilaça, Hao Chi Wong, Marshall Bern, Ricardo Dahab, and Antonio A. F. Loureiro. Secleach-on the security of clustered sensor networks. *Signal Process.*, 87(12):2882–2895, December 2007.

[17] Mathias Bohge and Wade Trappe. An authentication framework for hierarchical ad hoc sensor networks. In *Proceedings of the 2nd ACM workshop on Wireless security*, WiSe '03, pages 79–87, New York, NY, USA, 2003. ACM.

[18] Jie Tian, Guiling Wang, Tan Yan, and Wensheng Zhang. A power-efficient scheme for securing multicast in hierarchical sensor networks. In *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on*, pages 1–6, 2009.

[19] Manna Research Group and Project Sensornet. MannaSim Framework. `http://www.mannasim.dcc.ufmg.br/`. [Online; accessed February 20,2013].