Enhanced Chinese Remainder Theorem based Broadcast Authentication in Wireless Networks

Sonali S. Mhatre
Assistant Professor,
Information Technology,
University of Mumbai,
Mumbai-400032.

.Vandana B. Salve
Assistant Professor
Information Technology
University of Mumbai
Mumbai-400032

Sonali J. Mane
Assistant Professor
Information Technology,
University of Mumbai,
Mumbai-400032.

ABSTRACT
Wireless networks make extensive use of broadcast messages. Many routing activities and network management activities needed in wireless networks must rely on broadcast authentication mechanisms to ensure that data is being originated from a valid source. Without an efficient broadcast authentication algorithm, the transmitting node would have to resort to per-node unicast messages, which does not scale to large networks and is easy to compromise also. The goal of this work is to provide an efficient scheme for sensor network broadcast authentication by considering different properties of broadcast authentication. Here, a protocol is proposed Enhanced Chinese Remainder Theorem based Broadcast Authentication (ECRTBA), for wireless sensor networks. ECRTBA uses Chinese Remainder Theorem to associate the authenticating procedure of the authentication key and the Message Authentication Code of broadcast messages together. The important feature the scheme is having is that it uses the concept of independent keys which support infinite rounds of broadcasts. The scheme also provides instant authentication with no need of buffering.

General Terms
Wireless networks, Broadcast Authentication.

Keywords
CRT(Chinese Remainder Theorem), CRTBA(Chinese Remainder Theorem based Broadcast Authentication), ECRTBA (Enhanced Chinese Remainder Theorem based Broadcast Authentication), CAS(Certificate based authentication Scheme), (DAS) Direct storage based Authentication Scheme.

1. INTRODUCTION
In Wireless Networks, Broadcast communication is required in different areas:

1. Routing tree construction: AODV and DSR like protocol make use of broadcast RREQ packets for constructing routing tables.
2. Network management: Network management software require to network query to monitor the conditions.
3. To update the Software remotely broadcast authentication is required.
4. Need for time synchronization requires broadcast from time server.
5. To keep authorization information (grant/revoke) changing as per need, authenticated broadcasts are required.
6. Sensitive information broadcast

Many approaches have been suggested for broadcast authentication. However, objectively comparing such approaches and selecting the most appropriate one for a given application is a non-trivial process. Here are specified seven fundamental properties of broadcast authentication protocol [01]:

1. Resistance against node compromise

If sensor nodes are not equipped with tamper-proof or tamper-resistant hardware or software, any physical attacker would be able to physically compromise a node and obtain its cryptographic keys.

2. Low computation overhead

Some wireless nodes have limited computation resources, so an ideal protocol would have low computation overhead for both sender and receiver.

3. Low communication overhead

Radio communication consumes the most amount of energy, and thus protocols with high communication overhead are avoided if possible

4. Robustness to packet loss

Reliable message delivery is the property of a network such that valid messages are not dropped.

5. Immediate authentication

Depending on the application, authentication delay may influence the design of the wireless network protocol.

6. Messages sent at irregular times

Some applications send synchronous messages at regular and predictable times.

7. High message entropy

Many applications use messages of different sizes.

The different techniques available for broadcast authentication satisfy all but one property.

The purpose of this work is to understand those techniques and to suggest a better solution. Here, a new broadcast authentication technique ECRTBA (Enhanced Chinese remainder Theorem based Broadcast authentication) is proposed. It is modification of existing CRTBA (Chinese remainder Theorem based Broadcast authentication) to support unlimited rounds of broadcasts.

2. LITERATURE SURVEY
Authenticated broadcast requires an asymmetric mechanism. The traditional approach for asymmetric mechanisms is to use digital signatures, for example the RSA signature. Certificate based Authentication Scheme (CAS) [08] make use of Public/Private key pair and public key certificate issued by CA (Certificate Authority). In Direct storage based Authentication Scheme (DAS) [08] a node stores all the information of every other node including its public key. Unfortunately, asymmetric cryptographic mechanisms have high computation, communication, and storage overhead, making their usage on resource-constrained devices impractical for many applications. TESLA [02] is a lightweight broadcast authentication protocol, which use a one-way hash chain and the delayed disclosure of keys to provide the authentication service. However, it suffers from several drawbacks in terms of time synchronization and delayed authentication. Unlike TESLA, μTESLA uses multiple unicast for parameter distribution and hence is completely symmetric based [01]. Multilevel TESLA [05] uses higher level TESLA instances to distribute initial parameters. To facilitate

multiple rounds of broadcasts higher level TESLA instances are used. L-TESLA [7] was proposed to localize broadcast authentication by asking trusted nodes to maintain local TESLA key chains and re-authenticate broadcast packets in the name of the original source and asking sensor nodes to verify packets after receiving local TESLA keys from their nearby trusted nodes which helps in reducing verification delay. BABRA [04] (BAtch based BRoad cast Authentication) make use of independent keys associated with batches of packets. It does not use time synchronization but still has the problem of delayed authentication. Merkle hash tree [08] and Bloom filter [08] like techniques are based on asymmetric and thus are expensive in computation for resource constrained nodes. CRTBA [06](Chinese Remainder Theorem based Broadcast Authentication) make use of Chinese Remainder Theorem to send MAC of the message and authentication key bundled together in CRT unique solution. Table 1 describes the comparative analysis of the above discussed techniques.

Table 1 Comparative Study of existing Broadcast Authentication Techniques

	Node comp-romise	Compu-tation overhead	Commu-nication overhead	Robust-ness to packet loss	Instant authent-ication	Irregular message frequency	Message entropy	Hash Chain
TESLA	No	Less	During predistri-bution	Yes	No	No	Less	Yes
BABRA	No	Less	Less	Yes	No	Yes	Less	No
Merkle	No	Less	High	Yes	Yes	Yes	High	Yes
Enhanced Merkle	No	Less	Less	Yes	Yes	Yes	Less	Yes
Bloom filter	No	High	Less	Yes	Yes	Yes	Less	No
CAS	No	High	High	Yes	No	Yes	High	No
DAS	No	High	Less	Yes	Yes	Yes	Less	No
CRTBA	No	Less	Less	Yes	Yes	Yes	Less	Yes

3. BACKGROUND

CRTBA[06] scheme uses CRT to associate the authenticating procedure of the authentication key and the MAC of the broadcast message together. That is if the authentication key is authenticated, the MAC of the broadcast message has been authenticated too. To do these, we use CRT to map the MAC and the authentication key of the broadcast message to the CRT solution. The base station broadcasts the CRT solution and the broadcast message at the same time. When the receiver receives the CRT solution, it can recover the MAC of the message and the authentication key from the CRT solution using Chinese Remainder Theorem. To authenticate the authentication key, the receiver first uses a one-way hash chain of the authentication key to verify the authentication key. if the recovered authentication key is authentic, the CRT solution is authentic too. Then we use the CRT solution to verify the MAC of the broadcast message. The scheme satisfies many properties, including instant authentication, low overhead in computation, communication and storage, immunity against DoS attack. CRTBA first uses the one-way hash chain of the keys of to verify the authentication key and then use the authenticated CRT solution to verify the broadcast message. But use of key chain does not facilitate multiple rounds of broadcasts. The numbers of broadcast are limited by the length of the key chain. Use of very large key chain is also not recommended due to security reasons and also memory constraints.

3.1 Theorem 1 (Chinese Remainder Theorem)

Let $n_1, n_2, \ldots, n_k$ be pairwise relative primes, ie. GCD (n_i, n_j)=1, $i \neq j$. Let let $r_1, r_2, \ldots r_k$ be integers. Then the congruent equations

$x \equiv r_1 \bmod n_1$
$x \equiv r_2 \bmod n_2$
$x \equiv r_3 \bmod n_3$
….
$x \equiv r_k \bmod n_k$

have unique solution $x = \sum_{i=1}^{K} r_i N'_i N_i \pmod N$

where

$N = \pi_{i=1}^{K} n_i = n_1 n_2 \ldots n_k$

$N_i = \frac{N}{n_i}$

$N'_i = N_i^{-1} \pmod{n_i}$

Where $n_1, n_2 \ldots n_k$ are CRT moduli and x is the solution.

4. ECRTBA SCHEME

The basic idea of ECRTBA scheme is to use CRT to associate the authenticating procedure of the authentication key and the MAC of the broadcast message together. That is if the authentication key is authenticated, the MAC of the broadcast message has been authenticated too. To do this, existing algorithm uses CRT to map the MAC and the authentication key of the broadcast message to the CRT solution. Due to existence of key chain it supports limited rounds of broadcasts, but in the proposed algorithm we map the MAC computed using current authentication key, the key itself and hash of the next key to the CRT solution. The base station broadcasts the CRT solution and the broadcast message at the same time. When the receiver receives the CRT solution, it can recover the MAC of the message and the authentication key from the CRT solution using Chinese Remainder Theorem and store recovered hash of the next key to authenticate the next key. To verify the authentication key, the receiver first uses stored hash of the authentication key. If the recovered authentication key is authentic, the CRT solution is authentic too. Then we use the CRT solution to verify the MAC of the broadcast message.

4.1 Architecture

This scheme has three phases: the initialization procedure, broadcasting authentication packets, and authenticating broadcast packets.

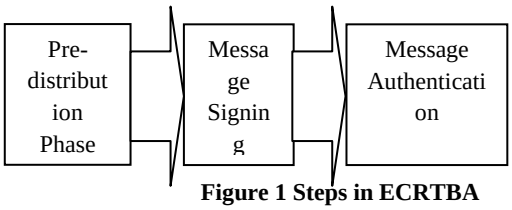

Figure 1 Steps in ECRTBA

4.2 Pre-distribution

Before the sensor nodes deployment, the base station executes the following steps:

Step 1: the base station generates a random key K_1

Step2: the base station randomly also generates three numbers n_1, n_2 and n_3 as the CRT *moduli*, and these three numbers are relative prime.

Setp3: the base station stores n_1, n_2, n_3 and $H(K_1)$ into each sensor memory using digital signature or multiple unicasts or bootstrapping the nodes.

4.3 Message signing

When the base station needs to broadcast message to sensor nodes, the base station must sign the message according the following method.

Figure 2 gives a detailed illustration of the CRTBA scheme message signing.

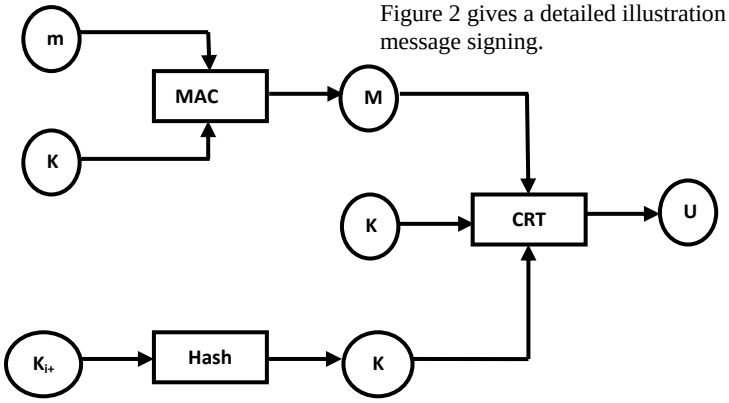

Figure 2 Enhanced CRTBA message signing

To sign the message *m*, the base station first computes the MAC of the message *m*, $M=MAC(m,Ki)$, hash of the next key $H(K_{i+1})$and then solves the congruent equation:

$U \equiv M \bmod n_1$
$U \equiv K_i \bmod n_2$
$U \equiv H(K_{i+1}) \bmod n_3$

After getting the congruent equation solution, the base station broadcasts message $<m,U>$ to all sensor nodes in the sensor networks.

4.4 Verification

After Sensor nodes have received the broadcast packets, they need to ensure that the broadcast packets come from the authenticated sensor. The sensor nodes verify the packets by the following way.

Figure 3 gives a detailed illustration of the CRTBA message authentication.

Step 1: The sensor nodes recover K_i from *U*, with *U* mod n_2. Then the sensor nodes need to check K_i correct by comparing whether hash of the received K_j is same as the one already received from the earlier message. If K_i is authentic, the sensor nodes recover *M*, with *U* mod n_1. Otherwise the received broadcast message has been modified.

Step 2: To verify message *m* integrity, the sensor nodes first compute the MAC of the broadcast using the authenticated key K_i and then compare $MAC(m, K_i)$ with *M* recovered from *U*. If $M=MAC(m,K_i)$, the message *m* is not tampered and then accepted; others the message *m* has been modified and the sensor nodes reject to accept the message *m*.

*Step 3:*The receiver recover hash of the next key by computing *U* mod n_3 and store it for verification of the key in the next broadcast message.

From the congruent equation, we can get the unique solution

$U = M N_1 N_1' + K_i N_2 N_2' + H(K_{i+1}) N_3 N_3' \bmod N$

Where,

$N= n_1n_2n_3 \quad N_1=N/n_2 \quad N_2=N/n_2 \quad N_3=N/n_3$

$N_1' = N_1^{-1} \bmod n_1$

$N_2' = N_2^{-1} \bmod n_2$

$N_3' = N_3^{-1} \bmod n_3$

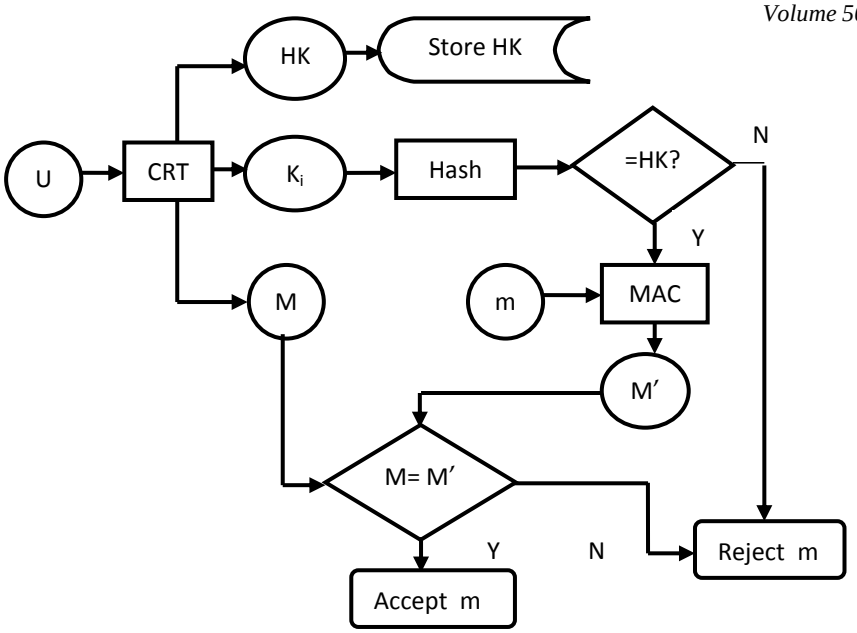

Figure 3 Enhanced CRTBA message authentication

Thus ECRTBA first use hash of the key of to verify the authentication key and then use the authenticated CRT solution to verify the broadcast message. The scheme satisfies many properties, including instant authentication, low overhead in computation, communication and storage, immunity against DoS attack and unlimited rounds of broadcasts.

5. ANALYSIS

ECRTBA scheme will now satisfy almost all the properties. It provides resistance against node compromise as it requires knowledge of the hash of the next key,. It is having low computation overhead, as Signature generation and verification requires just solving three congruent equations which involves three modulo inverse operations. It is having low communication overhead, since broadcast message just contains payload along with the CRT solution for congruent equations. It provides instant authentication as broadcast message itself carries the key. From the broadcast message pair $<m,U>$, Key K_i is derived by $U \bmod n_2$, then MAC of the message M is derived by $U \bmod n_1$. Then MAC M' is again computed using m and K_i. If the computed M' and M matches, the message is authentic. Hash of the next key is retrieved by $U \bmod n_2$ is stored for authentication of the key in the forthcoming message. Messages can be sent at irregular interval of times as it is not bound with time interval as in case of TESLA. Actual broadcast message and pre-distribution message both are too small. Actual broadcast message is $<m, U>$, where m is the payload and U is the solution to congruent equations and pre-distribution message is $<n_1, n_2, n_3, H(K_1)>$, where n_1, n_2 and n_3 are randomly generated keys and K_1 is the first.

6. RESULT

ECRTBA is been implemented on AODV (Ad-hoc On-demand Distance Vector Routing) Protocol and tested using NS-2.34 and Table 2 shows the result.

Table 2 Messages Sent and Received

Message	Sent HMAC of the message	Sent Current Key	Sent HMAC of the next key	Sent ECRT solution	Received HMAC of the message	Received current Key	Received HMAC of the next key
Computer Engineering	6	22	13	165295	6	22	13
Electronics Engineering	18	27	55	461581	18	27	55
Mechanical Engineering	57	35	61	268459	57	35	61
Chemical Engineering	50	50	43	184903	50	50	43
Automobile Engineering	62	41	25	322399	62	41	25
Civil Engineering	41	27	55	79771	41	27	55
Instrumentation Engineering	45	35	61	164329	45	35	61
Communication Engineering	31	50	14	237680	31	50	14
Electrical Engineering	26	35	43	258847	26	35	43

7. CONCLUSION

In this work, we implement efficient broadcast authentication scheme, ECRTBA, for wireless networks. In this scheme, we first use the hash of the of the authentication key of to verify the authentication key and then use the authenticated CRT solution to verify the broadcast message. The key feature of this new scheme is that it supports unlimited rounds of broadcasts which eliminate the need of pre-distribution of parameters after every certain number of broadcasts. Other features supported by this proposal includes instant authentication, low overhead in computation, communication and storage, immunity to DoS attack.

8. REFERENCES

[1] Mark Luk Adrian Perrig Bram Whillock Electrical and Computer Engineering Carnegie Mellon University, SASN'06, October 30, 2006, Alexandria, Virginia, USA, Seven Cardinal Properties of Sensor Network Broadcast Authentication, Copyright 2006 ACM 1-59593-554-1/06/0010

[2] Adrian Perrig Ran Canetti J. D. Tygar Dawn Song, The TESLA Broadcast Authentication Protocol

[3] Yongjie Fan, Ing-Ray Chen, and Mohamed Eltoweissy Department of Computer Science Virginia Tech, 2005, On Optimal Key Disclosure Interval for μTESLA: Analysis of Authentication Delay versus Network Cost 0-7803-9305-8/05/$20.00 ©2005 IEEE.

[4] Yun Zhou, and Yuguang Fang, 2006, BABRA: Batch-based Broadcast Authentication in Wireless Sensor Networks, 1-4244-0357-X/06/$20.00 © 2006 IEEE

[5] Donggang Liu Peng Ning, Multi-Level μTESLA: A Broadcast Authentication System for Distributed Sensor Networks

[6] Jianmin Zhang, Wenqi Yu, Xiande Liu, 2009, CRTBA: Chinese Remainder Theorem-Based Broadcast
\
Authentication in Wireless Sensor Networks, 978-1-4244-5273-6/09/$26.00 ©2009 IEEE

[7] Jawad Drissi and Qijun Gu., 2006, Localized broadcast authentication in large sensor networks in ICNS, July 2006.

[8] Xian Gan, Qiaoliang Li, 2009, A Multi-user DoS-containment Broadcast Authentication Scheme for Wireless Sensor Networks, 0018-9545/$26.00 © 2009 IEEE.

[9] Haowen Chan, Adrian Perrig Carnegie Mellon University Pittsburgh, Pennsylvania, USA, 2010, Round-Efficient Broadcast Authentication Protocols for Fixed Topology Classes IEEE Symposium on Security and Privacy

[10] Kui Ren, Member, IEEE, Shucheng Yu, Student Member, IEEE, Wenjing Lou, Senior Member, IEEE and Yanchao Zhang, Member, IEEE, 2009, Multi-User Broadcast Authentication in Wireless Sensor Networks, IEEE Transactions On Vehicular Technology, Vol. 58, No. 8, October 2009.

[11] Kui Ren, Member, IEEE, Wenjing Lou, Member, IEEE, Kai Zeng, Student Member, IEEE, And Patrick J. Moran, 2007, On Broadcast Authentication In Wireless Sensor Networks, IEEE Transactions On Wireless Communications, Vol. 6, No. 11, November 2007

[12] Qijun Gu Jawad Drissi, 2007, Dominating Set based Overhead Reduction for Broadcast Authentication in Large Sensor Networks, Third International Conference on Networking and Services(ICNS'07) 0-7695-2858-9/07 $20.00 © 2007

[13] Xian Gan, Qiaoliang Li, 2009, A Multi-user DoS-containment Broadcast Authentication Scheme for Wireless Sensor Networks, 978-0-7695-3688-0/09 $25.00 © 2009 IEEE DOI 10.1109/ITCS.2009.10