ISSN No. 0976-5697

Volume 4, No. 5, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Novel Secure Routing Protocol for Wireless Sensor Networks Using Binary Authentication Tree

B. Ganga Bhavani,Asst. Prof
Department of Computer Science,
B V C Engineering College, Odalaravu
E.G.Dt., AP, INIDA
e-mail: bhavanicse10@gmail.com

G L N V S Kumar, Asst. Prof
Department of M C A
B V C Institute of Technology & Science
Amalapuram, E.G.Dt., AP, INDIA
e-mail: kumar4248@gmail.com

R.V. Satyanarayan, Asso.Prof , HOD
Department of Computer Science,
B V C Engineering College, Odalaravu
E.G.Dt., AP, INIDA
e-mail: vsn_rayapureddy@yahoo.com

Abstract: In this paper, we propose a novel threshold key pre distribution scheme for wireless sensor networks by using symmetric keys to achieve authentication service. In the propose scheme called SRPWSN. Due to the fact that the wireless links in sensor networks are susceptible to attacks and the nodal mobility renders the network to have a highly dynamic topology it becomes critical to detect major attacks against the routing protocols of such networks and also provide some extent of QoS to the network traffic. In this we introduce new secure routing protocol (SRPWSN) with QoS routing mechanism. To achieve authentication service we use BAT scheme can effectively eliminate the performance bottleneck when verifying a mass of signatures within a required interval, even under adverse scenarios with bogus messages.

Keywords: Wireless sensor networks, key pre-distribution, Authentication, QoS, Binary authentication tree

I. INTRODUCTION

Security is a critical issue when sensor networks are deployed in a hostile environment. An essential security primitive, which is a building block for many security services, referred as key establishment. public key cryptography provides a complete solution in traditional networks.

Any public key infrastructure requires a trusted third party to distribute certificates. In the distribution of sensor nodes, so many nodes will not receive the entire information. To address this problem, there have been proposals for using symmetric cryptography or identity based signature scheme. In addition we use public-key-algorithm.

The routing protocol must be secured to defend attacks that may come from external (or) internal nodes In an external attack, a malicious node masquerades as a trusted node although it does not participate in routing process. It can generate floods of spurious service requests, such as Daniel Of Service(DOS) attack. So it is more difficult to detect the internal attacks, second protocol must be integrated with QoS routing schemes to support the QoS requirements of the carried traffic.

The existing security routing protocol for wireless sensor networks often avoid either most challenging internal attacks (or) QoS requirements of the traffic.

To provide more security and performance issues, we introduce robust and efficient signature scheme, call a Binary Authentication Tree(BAT).

Robustness: The BAT scheme is competent for adverse attack scenario with bogus messages, then each router can quickly distinguish the bogus messages from all the authentic ones. Therefore, our BAT scheme can efficiently tolerate, to a large extent ,message flooding attacks.

Efficiency: The BAT scheme efficiently eliminates the performance bottleneck due to the significantly reduced computational overhead. To verify any n received messages with k>=1 bogus ones. the number of time consuming pairing operations in approximately equal to (k+1).log(n/k)+4k-2.In ideal case(k=0),the computation overhead to verify all the messages can be remarkably reduced from 2n-time consuming pairing operations to 2.

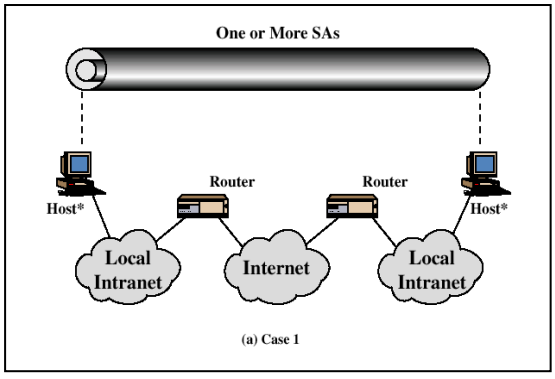
BAT scheme is the first one to include evaluated theoretical boundaries of verification complexity for the batch verification of identity-based signatures under attacks which can be used to guide the balance between security and performance.

II. RELATED WORK:

The existing SRPs for wireless sensor networks can be divided into two categories: in terms of how SRP is secured and what types of attacks it can defend.

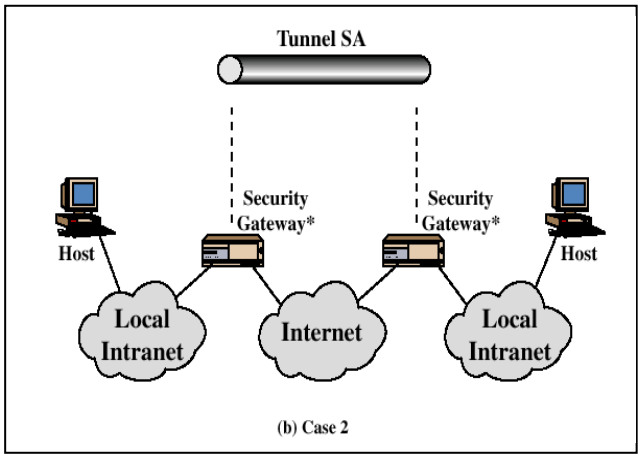
In the first category ,we use a method is to establish a security association between source and destination nodes by using routing protocols AODV,DSR and DSDV can be secured. By using one-way hash chains to provide authentication to defend attacks that modify routing information.

CASE(i):All security is provided between end systems that implement IPSec.

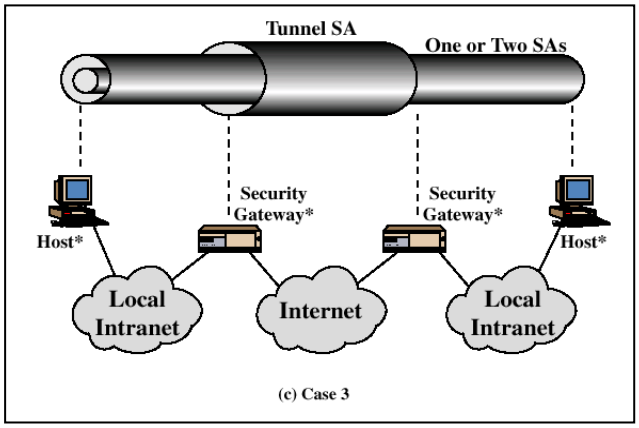


CASE(ii):security is provided only between gateways.

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 25-26 March 2013
Organized by
Vignan University, India



CASE(iii):adding end-end system to case (ii)



In the second category ,the major purpose is to protect routing traffic against the internal attacks, the authors proposed to use both route and message redundancy to detect different copies of message received over different routes.

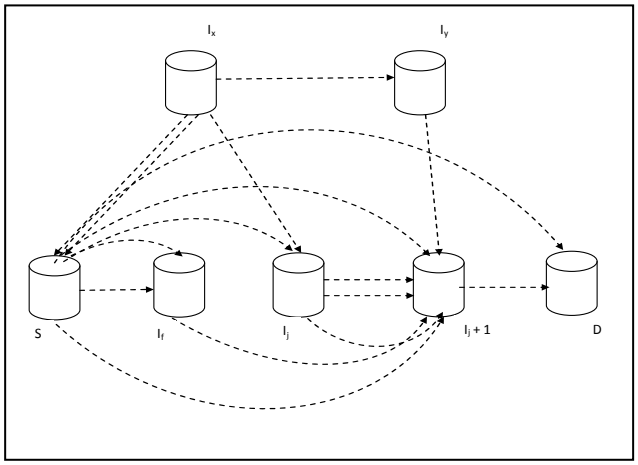


Fig: Multiple copies of ménage forward over different routes

IV. NOTATIONS AND DESCRIPTIONS

Notation	Descriptions
S	The private master key of TA
P_{Pub}	The public keyof TA
ID_i	The real identity of the router
Sk_i	A private key of the router
||	Message concatenation operator
h(.)	A one=way hash function such the MD5 (OR)SHA-1
$E_K(.)$	Symmetric encryption with key k
$D_K(.)$	Symmetric decryption with key k
I_i	I^{th} router
M_i	A message sent by the router i
A_i	A signature sent by the router i

V. PRELIMINARIES:

The following figure shows the application scenario model represents the identity –based cryptography using BAT scheme.

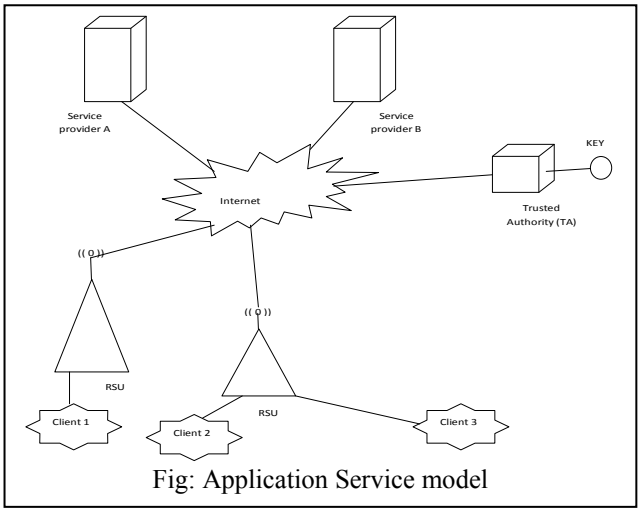


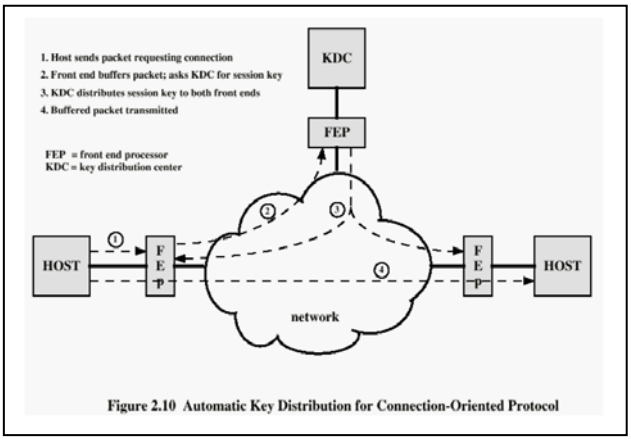
Fig: Application Service model

RSU:RSU serves as a gateway connecting the clients within its transmission range to the internet.

Clients: all clients exchanges messages with the RSU within its range. Each client is equipped with sensing and processing units.

Trusted Authority (TA): The TA server, as the key distribution centre, is responsible for generating and assigning related parameters for the clients and RSUs

Service provider (SP): The SP (or) application server is responsible for collecting the traffic related information such as congestion, overloading etc.



Identity based cryptography(IBC) IBC is a type of public-key cryptography in which the public key of a user is his/her unique identity information. in this we use RSA algorithm.

Bilinear Pairing: Let G and GT be group and cyclic multiplicative group generated by p with the same prime order q.

$|G|=|GT|=q$

Bilinear map has the following properties.

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 25-26 March 2013
Organized by
Vignan University, India

(i)Bilinear:
V P, Q, R □ G and V a, b □ z, than
eˆ(ap, bp) = eˆ(p, bp)a = eˆ(ap, p)b = eˆ(p,p)ab

(ii) Non degenerate:
□P, Q □ G such that eˆ(P, Q) ≠ /GT.

(iii)computable:
V P, Q □ G, there is efficient alg. To calculate eˆ(P,Q)

Providing authentication service by using Binary authentication tree:

Message authentication code is the one-way hash function. As with the message authentication code, a hash function accepts a variable size message M as input and produces a fixed size message digest H(M) as output.

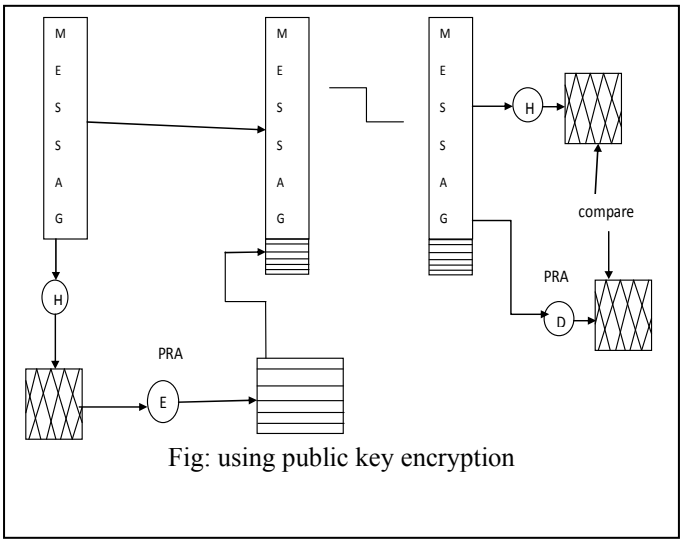


Fig: using public key encryption

We can use signature scheme by using IBC. It contains four basic terms.

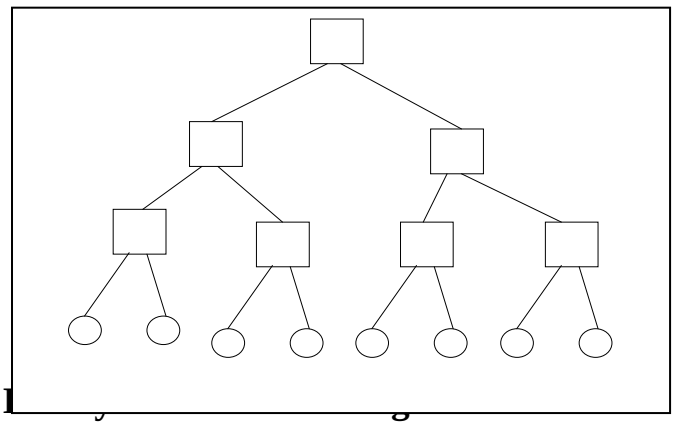
(i) Setup: in this we use MD-5 algorithm.

(ii) Extract: we can extract the information from various nodes.

(iii) Sign: by using DSRC protocol we create the signature and append that signature to the message and transfer the message along with signature to the destination.

(iv) Verify: on receiving message we can apply hash function that produce message digest and compare with the receiving message digest and verify it.

Binary authentication tree:



Algorithm: 1 fast check

Binary authentication algorithm:

Algorithm: 1 fast check

01: fast check ()

02: {

03: k1=2h-l..V, k2=2h-l.(v+1)-1

$K2$ $K2$

04: if eˆ(Σ Fi, p)= eˆ{ Σ [Ei(Mi, Ei) H (PII)], P pub}

$I=K_1$ I=K1

05: return TRUE;

06: else

07: return FALSE

08 :}

Algorithm: 2 Binary authentication

01: binary_auth ()

02: {

03 :if(fast_check()=TRUE

04 : return FS

05: if l=h

06 :return FS=FS U{œ < h, v >};

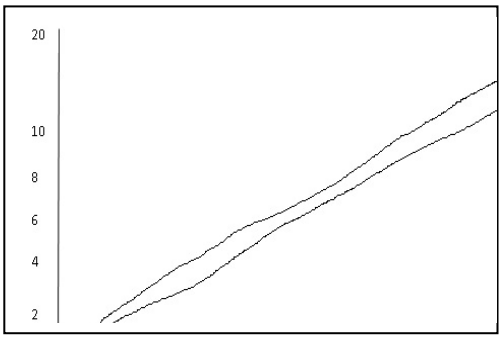
//finding fake signature//

07 : return binary_auth(œ < l+1,2 v >Fs)

08:return binary_auth (œ < l+1,2v+1 >Fs)

09:}

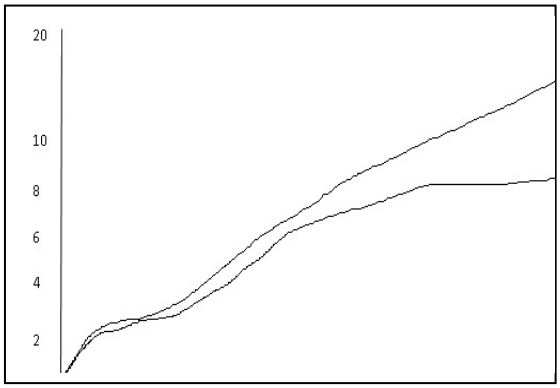
Simulation results:



We simulate the proposed SRP protocol in wireless sensor networks by using NS-2 simulator.

Simulation results:

By using proposed protocol we can deliver the packets in the presence of 20 malicious nodes with 50 nodes.



CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 25-26 March 2013
Organized by
Vignan University, India

The total number of packets delivered in the presence of 20 malicious nodes in a network with 50 nodes with more authentication service.

VI. CONCLUSION

In this paper, we address the most challenging problem of designing a secure routing protocol with QoS support. for a routing protocol to detect the major internal attacks, we propose both route and message redundancies during topology discovery. For each and every incoming message we can apply authentication service by using binary authentication tree.

VII. REFERENCES

[1] J. Postel, "RFC793—transmission control protocol," *RFC*, 1981.

[2] C. Lochert, B. Scheuermann, and M. Mauve, "A survey on congestioncontrol for mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 7, no. 5, p. 655, 2007.

[3] J. Postel, "RFC791—Internet Protocol," *RFC*, 1981.

[4] A. Al Hanbali, E. Altman, and P. Nain, "A survey of TCP over ad hoc networks," *IEEE Commun. Surveys Tutorials*, vol. 7, no. 3, pp. 22–36, 3rd quarter 2005.

[5] J. Widmer, R. Denda, and M. Mauve, "A survey on TCP-friendly congestion control," *IEEE Network*, vol. 15, no. 3, pp. 28–37, May/June 2001.

[6] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, "A comparison of mechanisms for improving TCP performance over wireless links," *IEEE/ACM Trans. Netw.*, vol. 5, no. 6, pp. 756–769, December 1997.

[7] K.-C. Leung, V. Li, and D. Yang, "An overview of packet reordering in transmission control protocol (TCP): problems, solutions, and challenges," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 4, pp. 522–535, April 2007.

[8] S. Low, F. Paganini, and J. Doyle, "Internet congestion control," *IEEE Control Syst. Mag.*, vol. 22, no. 1, pp. 28–43, February 2002.

[9] G. Hasegawa and M. Murata, "Survey on fairness issues in TCP congestion control mechanisms," *IEICE Trans. Commun. (Special Issue on New Developments on QoS Technologies for Information Networks)*, vol. E84-B, no. 6, pp. 1461–1472, June 2001.

[10] M. Gerla and L. Kleinrock, "Flow control: a comparative survey," *IEEE Trans. Commun.*, vol. 28, no. 4, pp. 553–574, April 1980.

[11] J. Nagle, "RFC896—Congestion control in IP/TCP internetworks," *RFC*, 1984.

[12] C. A. Kent and J. C. Mogul, "Fragmentation considered harmful," in *Proceedings of the ACM workshop on Frontiers in computer communication technology (SIGCOMM)*, Stowe, Vermont, August 1987

CONFERENCE PAPER
"National Conference on Networks and Soft Computing"
On 25-26 March 2013
Organized by
Vignan University, India