A Novel Energy Efficient Authentic Reliable Routing Protocol (EEARRP) for Scalable Mobile Ad Hoc Networks

R.Vadivel
Assistant Professor,
Department of Information Technology,
School of CSE, Bharathiar University
Coimbatore 641 046.

B.Narasimhan
Assistant Professor,
Department of Computer Technology,
Dr. N.G.P. Arts and Science College,
(Affiliated to Bharathiar University),
Coimbatore 641 048.

ABSTRACT
This paper proposes a novel energy efficient authentic reliable routing protocol (EEARRP) to attain better authenticity in scalable mobile ad hoc networks. To decrease the signature verification expenditure and message communication expenditure a mechanism with message recovery is employed. The proposed authentic scheme is to minimize the size of the message transmitted when the signature length is reduced any more. To implement this, the energy efficient authentic reliable routing scheme with message recovery is used. Therefore, the communication overhead is minimized guaranteed in the above said scheme. The total length of the broadcast message is reduced by 24%. As a result, the total energy consumption of our scheme can be reduced by up to 27%. With the extensive simulation results using NS2 the proposed EEARRP attains better throughput, packet delivery ratio with reasonable decrease in total energy consumption and total overhead even in real-time scalable environment.

Keywords
Reliability, Energy Efficient Routing, Authenticity, Scalability, Mobile ad hoc networks.

1. INTRODUCTION
In general, a mobile ad hoc network (MANET) is self-possessed of a dynamic set of nodes which rely on each other to relay packets due to the lack of a fixed networking infrastructure. MANETs have been widely used in a variety of military scenarios, such as soldiers exchanging information for situational awareness on the battlefield, search teams coordinating in combat search and rescue efforts, and real-time enemy detection around a troop station. Compared with traditional infrastructure-based networks, MANETs are more susceptible to malicious attacks and random failures due to their unique features such as constrained node energy, error-prone communication media, and dynamic network topology. Therefore, energy efficient along with security is a key concern for MANETs. Security threats in MANETs come from both malfunction of mobile devices and subversion to these devices by enemies.

1.1. Problem Statement

Adaptive authentication and energy management is very significant for mobile ad hoc networks because mobile nodes are usually battery-powered. Energy efficient control mechanisms have the possibility to decrease mobile nodes energy consumption and further increase the network lifetime. Also providing authentication along with energy efficient routing is a challenging task in mobile ad hoc networks. A lot of researchers have been paying attention for designing and developing authentic and energy efficient routing strategies. In this paper we propose a novel energy efficient and authentic reliable routing protocol for scalable mobile ad hoc networks. The energy efficient routing is attained by reducing the overhead packets incurred while authentication.

2. LITERATURE REVIEW
The TESLA scheme [9] is well known for its ability to provide source authentication and message integrity by utilizing a one-way hash chain and loose time synchronization between a sender and receivers. However, it has limited scalability due to its unicast-based parameter distribution to add new receivers. Subsequently, the multilevel TESLA [8] was proposed to enhance the scalability of the TESLA scheme.

These TESLA-like schemes [9,8,15,7,10,18,16] are associated with large buffers due to the delayed authentication of the messages, which can easily lead to severe energy-depleting DoS attacks. sThe schemes based on symmetric key techniques fare attractive in terms of their energy efficiency, but a secret key distribution problem between senders and receivers is the most serious obstacle. On the other hand, BA schemes based on public key cryptography (PKC) [12,6,1,13] can eliminate this key distribution problem.

Recent works [2,12] have shown that many well-known PKC schemes are acceptable for sensor nodes: it was reported that on an Atmel ATmega 128 at 8 MHz, a 160-bit ECC point multiplication took only 0.81 s (second). However, the use of certificates in the Public Key Infrastructure (PKI) consumes substantial bandwidth and power due to the transmission and verification of public key certificates. Therefore, PKI is considered to be unsuitable for WSN, although it can provide greatly simplified and stronger security solutions.

Oliveira et al. [4] showed how short signatures from pairings by Boneh et al. [19] can be used to authenticate sensors in aWSN and Galindo et al. [14] used TinyPBC to make explicit the benefits of using PBC to solve the key distribution problem in underwater WSNs.

More recently, with TinyPBC [5], the gT pairing could be computed in 1.9 s, 1.27 s and 0.46 s on the ATmega 128L, the MSP430 and PXA27x platforms, respectively. The above results show that, the time needed to compute a pairing computation in sensor nodes has increased by 5 times over the past 3 years. Currently, a pairing can be computed in about 0.5 ms on an AMD Phenom II X4 940, 3.0 GHz [1]. Furthermore, next-generation sensor nodes such as the

Heliomote node [13] are expected to facilitate a continuous energy supply to nodes by deriving their power from solar sources. Therefore, we can expect wider acceptance of PBC for WSNs in the near future. Recently, Ren et al. [3] proposed an ID-based BA scheme based on Hess's ID-based signature (IBS) scheme [11].

Although the broadcast message size can be reduced owing to the elimination of public key certificates for users, this scheme has very high computational overhead, as two pairing computations and a MapToPoint operation are required for each sensor node, where the MapToPoint function is used to map identity information onto a point on an elliptic curve.

Cao et al. [17] proposed a more efficient ID-based multi-user BA scheme, IMBAS, based on a pairing-free IBS scheme. The signature scheme requires neither a pairing computation nor the MapToPoint function for verification, while its resulting signature consists of two elements of the underlying group and a 160-bit hash value at an 80-bit security level. Compared to Ren et al.'s scheme, its verification efficiency is improved, but its signature length is about 30% longer.

3. PROPOSED WORK

This paper we propose a mechanism to reduce the total energy consumption of mobile nodes that are present in the mobile ad hoc network. This is achieved by minimizing the total length of the broadcast message. Taking into account of to energy expenditure the communication overhead is greater than calculation overhead. Communication delay has not yet improved considerably even though advancement of arithmetic calculations is done. In this research work we propose an energy efficient authentic reliable routing protocol for scalable mobile ad hoc networks. To perk up the signature verification expenditure and communication expenditure a mechanism with message recovery is employed. The key idea is to reduce the size of the message transmitted when the signature length is reduced any more. To implement this, the energy efficient authentic reliable routing scheme with message recovery is used. Therefore, the communication overhead is minimized guaranteed in the above said scheme. The total length of the broadcast message is reduced by 24 %. As a result, the total energy consumption of our scheme can be reduced by up to 27%. The proposed routing protocol EEARRP is compared to the scheme in as in [7].

The proposed EEARRP scheme consists of four stages. They are system initial process, adaptive private key extraction, generating signature and signature verification.

3.1 System initial process

Before deploying the mobile ad hoc networks, a destination mobile node creates the system parameters as follows:

- $C \in B^+$, generate a prime p, two groups J_1 and J_2 of order p, a generator $Q \in J_1$, and a bilinear pairing $f : J_1 \times J_1 \rightarrow J_2$.
- Choose a random $a \in bB_p^*$ and set $MPK = SM$ as a master public key and master secret. Compute $f(Q,Q)^{-1}$ and set $\mu = f(Q,Q)^{-1}$.
- Choose four cryptographic hash functions $\left[N : \{0,1\}^* \rightarrow B_p^*, N_1 : \{0,1\}^* \rightarrow \{0,1\}^{l_1+l_2}, \right.$ $\left. X1 : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2} \; and X2 : \{0,1\}^{l_2} \rightarrow \{0,1\}^{l_1} \right]$ and where $|p| = l_1 + l_2$.
- The system parameters *paras*={J1,J2,f,p,Q,MPK, μ , X_1,X_2, l_1, l_2}.

These public system parameters, *paras*, are preloaded in each mobile node consisting of mobile ad hoc networks.

3.2 Adaptive private key generation

When a user in the mobile nodes with an identity $ID \in \{0,1\}^*$ wants to join the mobile ad hoc network, it has to obtain its private key generated by the destination node. When the user requests its private key, the destination node calculates the user's private key as

$SK = \frac{1}{N(id) + a} Q$ corresponding to ID_i.

It is a noteworthy fact that ID_i's the public key required during the verification process is $MPK + N(id_i)Q$. The destination node sends the private key SKi to the user pass through a secure channel and the user stores it in its tamper-proof device.

3.3 Generating signature

When a user wants to broadcast a message to the mobile ad hoc network, it signs a message using the proposed authentication scheme. To sign a message $MSG \in \{0,1\}l^{1_1}$, the network user with a private key SK_i corresponding to ID_i finishes the following steps:

1. Pick the current Time_Stamp TS_i
2. Choose $h_1 \in bB_p^*$ and compute μ^{h_1} and $\alpha = N_1(ID_i, TS_i, \mu^{h_1}) \in (0,1)l_1 + l_2$
3. Compute $\beta = X_1(MSG) \| (X_2(X_1(MSG)) \oplus MSG), h_2 = [\alpha \oplus \beta]_{10}$ and $U = (h_1 + h_2)SK_i$. Then $\sigma_i = (h_2, U)$ is a signature on MSG for ID_i.

The user then broadcasts <ID_i,TS_i, σ > in the mobile ad hoc network, where ID_i and TS_i are taken to be two bytes.

3.4 Signature Verification

On the reception of <ID_i,TS_i, σ >, each mobile node checks its authenticity. It first checks whether the timestamp TS_i is valid or not. Assuming that δ is the predefined message propagation time limit, we should have TS $\overline{TS}_i \leq \delta$. Then, for the sender node's identity ID_i, the mobile node looks up the revocation list in its local storage to determine the corresponding entry. If it exists, the broadcast message is discarded, as it was generated by a network user with a revoked ID_i. If TS_i is fresh and ID_i is not in the revocation list, the mobile node proceeds with the following signature verification:

$$\tilde{\alpha} = N_1(ID_i, TS_i,$$

1. Compute $p(U, N, (ID_i)Q + MPK).\mu^{h_2}$

$$and\ \tilde{\beta} = [h_2]_2 \oplus \tilde{\alpha}$$

2. Recover the message

$\overline{MSG} = \left|\tilde{\beta}\right| l_1 \oplus X_2(l_2 \left|\tilde{\beta}\right|)$ and

accept σ as a valid signature of the broadcast message

$\tilde{MSG}(= MSG)$ if and only if

$l_2 \left|\tilde{\beta}\right| = X_1\left(\tilde{MSG}\right)$.

If this verification process fails, the mobile node discards the message. Otherwise, the authenticity of the received message is guaranteed. Signature verification in this phase requires only one pairing computation, a scalar multiplication in J_1, and an exponentiation in J_2

4. SIMULATION SETTINGS AND PERFORMANCE METRICS

Table1. Simulation settings and parameters

No. of Nodes	25, 50, 75, 100, 125, 150, 175, 200, 225 and 250
Area Size	1500 X 1500 meters
MAC	802.11b
Radio Range	250 meters
Simulation Time	100 seconds
Traffic Source	CBR
Packet Size	512 KB
Mobility Model	Random Waypoint Model
Speed	5 m/s
Initial Energy	2.0 Joules

Performance metrics

The performance metrics such as throughput, delivery ratio, energy expenditure and overhead are taken into account for simulation.

5. RESULTS AND DISCUSSIONS

From Figure.1 it can be seen that the proposed routing protocol EEARRP achieves better throughput than that of the conventional protocol AODV. Also it can be analyzed from Figure.2 that the packet delivery ratio of the proposed routing protocol EEARRP maintains the delivery ratio in a stable manner even at scalable conditions. In Figure.3 the energy expenditure of the proposed EEARRP Vs AODV is shown. From the simulation it shows that EEARRP is comparatively consuming less energy than that of AODV routing protocol. In Figure.4 the comparison is carried out for overhead packets delivered by the nodes in a scalable ad hoc network environment. Extensive simulation results shows that the proposed EEARRP consumes lesser overhead when compared with the existing routing protocol such as AODV.

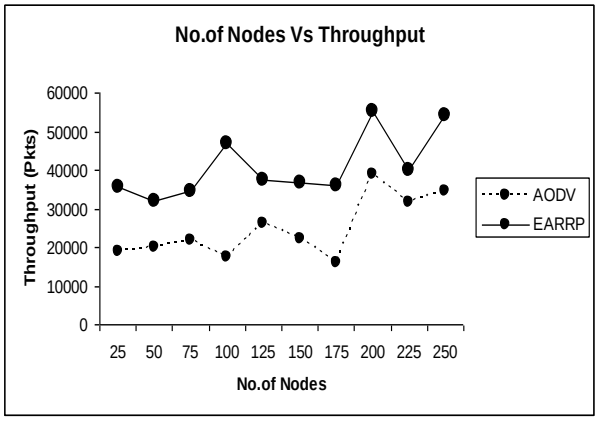

Fig.1 No. of Nodes Vs Throughput

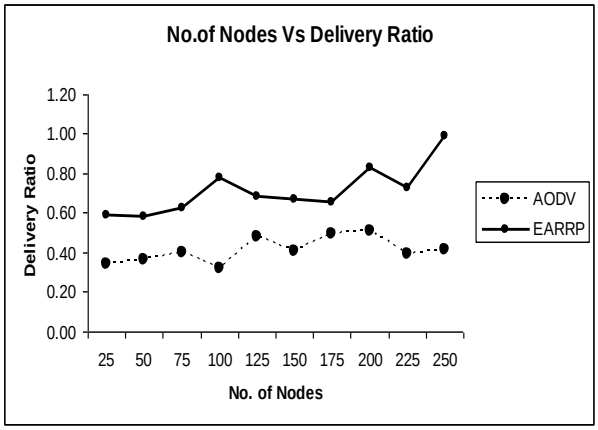

Fig.2 No.of Nodes Vs Delivery Ratio

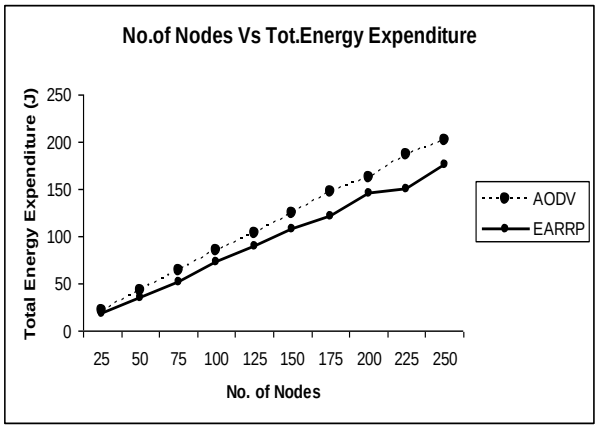

Fig.3. No.of Nodes Vs Total Energy Expenditure

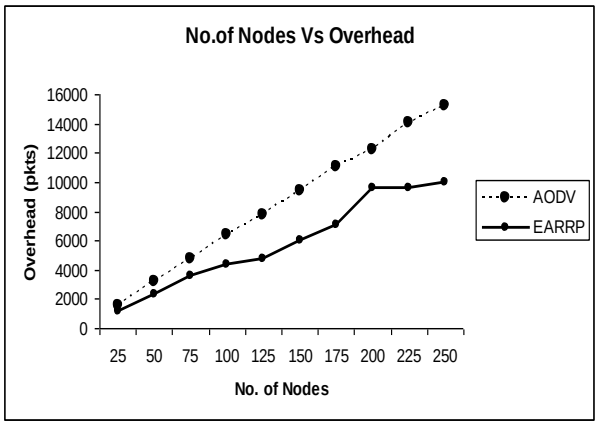

Fig.4. No.of Nodes Vs Overhead

6. CONCLUSIONS

In this paper, we presented a novel energy efficient authentic reliable routing protocol (EEARRP) in order to attain better authenticity in scalable mobile ad hoc networks along with reduced energy consumption. To decrease the signature verification expenditure and message communication expenditure a mechanism with message recovery is proposed. The proposed authentic scheme minimizes the size of the message transmitted when the signature length is reduced any more. To implement this, the energy efficient authentic reliable routing scheme with message recovery is used. Therefore, the communication overhead is minimized guaranteed in the above said scheme. The total length of the broadcast message is reduced by 24%. As a result, the total energy consumption of our scheme can be reduced by up to 27%. With the extensive simulation results using NS2 the proposed EEARRP attains better throughput, packet delivery ratio with reasonable decrease in total energy consumption and total overhead even in real-time scalable environment.

7. ACKNOWLEDGEMENTS

The first author thanks UGC for allocating Minor Research Project grant during Feb 2011 to Feb 2013 Grant 39-947/2010 (SR). The second author thanks the management of Dr.N.G.P. Educational Institutions for providing career opportunity as Assistant Professor in the Department of Computer Technology at Dr. N.G,P. Arts and Science College, Coimbatore.

8. REFERENCES

[1] H. Wang, Q. Li, Efficient implementation of public key cryptosystems on mote sensors, in: Proceedings of ICICS'06, 2006, pp. 519–528.

[2] A.S. Wander, N. Gura, H. Eberle, V. Gupta, S.C. Shantz, Energy analysis of public-key cryptography for wireless sensor networks, pervasive computing and communications, in: Proceedings of PerCom'05, 2005, pp. 324–328.

[3] K. Ren, K. Zeng, W. Lou, P. Moran, On broadcast authentication in wireless sensor networks, IEEE Transactions on Wireless Communications 6 (11) (2007) 4136–4144.

[4] L.B. Oliveira, A. Kansal, B. Priyantha, M. Goraczko, F. Zhao, Secure-TWS: authenticating node to multi-user communication in shared sensor networks, in: Proceedings of IPSN'08, 2009, pp. 289–300.

[5] L.B. Oliveira, D.F. Aranha, C. Gouvea, M. Scott, D. Camara, J. Lopez, R.Dahab, TinyPBC: pairings for authenticated identity-based noninteractive key distribution in sensor networks, Computer Communications 34 (3) (2011) 485–493.

[6] D. Malan, M. Welsh, M. Smith, A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography, in: Proceedings of SECON'04, 2004, pp. 71–80.

[7] D. Liu, P. Ning, S. Zhu, S. Jajodia, Practical broadcast authentication in sensor networks, in: Proceedings of MobiQuitous'05, 2005, pp. 118–132.

[8] D. Liu, P. Ning, Multi-level lTESLA: broadcast authentication for distributed sensor networks, ACM Transactions of Embedded Computing Systems 3 (4) (2004) 800–836.

[9] D. Liu, P. Ning, Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks, in: Proceedings of NDSS'03, 2003, pp. 263–276.

[10] T.K. Kwon, J. Hong, Secure and efficient broadcast authentication in wireless sensor networks, IEEE Transactions on Computers 59 (8) (2010) 1120–1133.

[11] F. Hess, Efficient identity based signature schemes based on pairings, in: Proceedings of SAC'02, LNCS 2595, Springer-Verlag, 2003, pp. 310–324.

[12] N. Gura, A. Patel, A. Wander, H. Eberle, S.C. Shantz, Comparing elliptic curve cryptography and RSA on 8-bit CPUs, in: Proceedings of CHES'04, 2004, pp. 119–132.

[13] G. Gaubatz, J. Kaps, B. Sunar, Public key cryptography in sensor networks-revisited, in: Proceedings of 1st European Workshop on Security in Ad-Hoc and Sensor Networks, LNCS 3313, Springer- Verlag, 2005, pp. 2–18.

[14] D. Galindo, R. Roman, J. Lopez, A killer application for pairings: authenticated key establishment in underwater wireless sensor networks, in: Proceedings of CANS'08, LNCS 5339, Springer, 2008, pp. 120–132.

[15] J. Drissi, Q. Gu, Localized broadcast authentication in large sensor networks, in: Proceeding of ICNS'06, 2007, pp. 341–350.

[16] S. Cheng, An efficient message authentication scheme for link state routing, in: Proceedings of ACSAC'97, 1997, pp. 90–98.

[17] X. Cao, W. Kou, L. Dang, B. Zhao, IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks, Computer communications 31 (14) (2008) 659–667.

[18] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, Multicast security: a taxanomy and some efficient constructions, in: Proceedings of INFOCOMM'99, 1999, pp. 708–710.

[19] D. Boneh, B. Lynn, H. Schacham, Short signatures from the weil pairing, Journal of Cryptology 17 (4) (2004) 297–319.

[20] D.F. Aranha, K. Karabina, P. Longa, C.H. Gebotys, J. Lopez, Faster explicit formulas for computing pairings over ordinary curves, in: Proceedings of Eurocrypt'11, LNCS 6632, Springer-Verlag, 2011, pp. 8–68.