ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Energy Conscious Privacy Preserving Security System for MANETs

A.Naveena[1], Dr.K.Rama Linga Reddy[2]

Asst. Professor, Dept. of ETM., G. Narayanamma Institute of Technology and Science, Hyderabad, India[1]

Professor, HOD, Dept. of ETM, G. Narayanamma Institute of Technology and Science, Hyderabad, India[2]

ABSTRACT: In the present world, Mobile Adhoc Networks have become very prominent. Security is needed not only for data but also for nodes. Security is a challenging factor for these MANETs. Offering Security and privacy preservation is an important research issue is MANETs which have power constraints. Node privacy is possible by implementing anonymous routing protocols.Till now proposed Anonymous Routing Protocols achieved security in adverse environment but with less efficiency with regard to power constraints. In this paper, a Hybrid Security System is proposed which combines modified zero knowledge proof, bloom filter and elliptic curve cryptographic techniques. The proposed hybrid system implements Lightweight Energy Efficient Anonymous Routing Protocol and its efficiency is determined by simulation using NS2.

KEYWORDS: Anonymity, Bloom filter, ECC, Energy Conscious,Privacy Preservation,Pseudonymity, ZKP.

I. INTRODUCTION

Mobile adhoc networks do not depend on any centralized infrastructure. They are self-maintained networks which requires cooperation among peer nodes. Hence security is a challenging issue. Existing Anonymous Routing protocols provide node anonymity and security but with less efficiency [1],[2],[3],[4],

Security mechanisms can be added to existing routing protocols to resist attacks. Cryptographic techniques are used to ensure the authenticity and integrity of routing messages [5]. A major concern is the tradeoff between security and performance, given the limited resources available at many MANET nodes. Both symmetric and asymmetric cryptography have been used as well as hash chaining.

Hybrid security system presented in this paper implements a light weight energy efficient Anonymous Routing protocol which combines zero knowledge proof, bloom filter and Elliptic curve cryptography techniques to achieve energy efficiency and security. The rest of the paper is organized as follows. In section II, Related work. Proposed System Model is discussed in Section III. Section IV andV deal with Protocol and Performance Evaluation respectively. Section VI deals with conclusion.

II. RELATED WORK

Survey shows that, the Anonymous On –Demand Routing (ANODR)[6] , uses one time public and private key to achieve anonymity but failed to achieved proper content unobservability. The Anonymous Location Aided Routing (ALARM) [7] provided secured communication against adversaries but failed to provide location anonymity. This was overcomed by ALERT [8] protocol but it failed to provide node authentication. AASR [9] protocol provided anonymity and security against attacks but with more energy consumption. SDAR [10] protocol also allowed trustworthy intermediate nodes to participate in path formation.

III. PROPOSED SYSTEM MODEL

Proposed System Model presents brief description about network model, adversary model, bloom filter and zero knowledge proofand it is depicted in Fig1

DOI: 10.15680/IJIRCCE.2016. 0411149

A. ***CREATION OF NETWORK MODEL***

In the creation of Network Model, a dynamic network with N set of nodes and R set of router for set of pairs (n_i, nj) is considered. Data is forwarded from source node n_i to destination node n_j with the help of neighbor nodes nk.

B. ***IMPLEMENTATION OF BLOOM FILTER***

A bloom filter is a data structure which can store the elements of a set in a space efficient manner. It uses a set of elements X ={X1, X2,X3………. Xn}, with an array of n bits and m independent hash functions hi ={h1, h2, h3……. Hn} with range {1,…….m}. It is used to identify route loops.

C. ***DESIGN OF ADVERSARY MODEL***

Due to mobility and absence of centralized infrastructure, MANETs are easily compromised with attacks. In MANETs, communication is not highly reliable due to resource constraints. These attacks can be either passive or active. Both the attacks are analyzed to ensure reliability and security.

D. ***MODIFIED ZERO KNOWLEDGE PROOF.***

A zero –knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true [11]. It has three properties.

i. Completeness
ii. Soundness
iii. Zero-knowledge

If also has additional properties like randomness and timing.

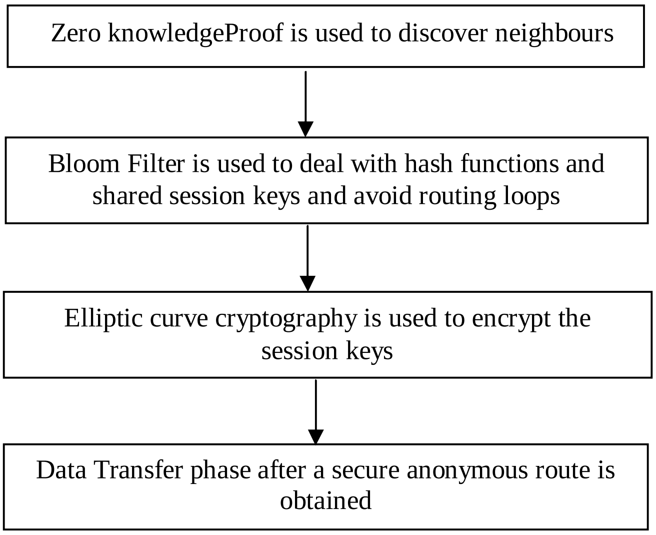

Zero knowledgeProof is used to discover neighbours
Bloom Filter is used to deal with hash functions and shared session keys and avoid routing loops
Elliptic curve cryptography is used to encrypt the session keys
Data Transfer phase after a secure anonymous route is obtained

Fig 1: Data flow diagram of proposed Hybrid Security System

E.After designing all the above models the system is implemented in different phases.

i .*Anonymous Route discovery phase*

The source node n_j sends RREQ message to communicate with the destination node n_j. The RREQ message consists of message type, RREQ, message id and sequence number. Computation of hash function is done with the help of bloom filter and the shared session keys are $h(k_1)$, $h(k_2)$, ………………….. $h(k_n)$. Then real destination is identified and verified using Elliptic curve cryptographic technique [12].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

ii.*Route Reply Phase*

The destination node n_j replies to the source node n_i for the corresponding RREQ message. The destination node verifies the node authentication and sends route reply message to the source node.

iii. Data Transfer Phase

After the anonymous route discovery phase and route phase are completed, data transfer place to achieve confidentiality.

IV. PROPOSED SYSTEM EVALUATION

Security and Energy parameters are considered to determine the efficiency of the proposed system.

A. ANONYMITY AND SECURITY

The proposed hybrid security model, reduces fake routing packets and since sequence numbers are used, reply attacks are not possible. It provides a good defense against DOS attacks.

B. ENERGY EFFICIENCY

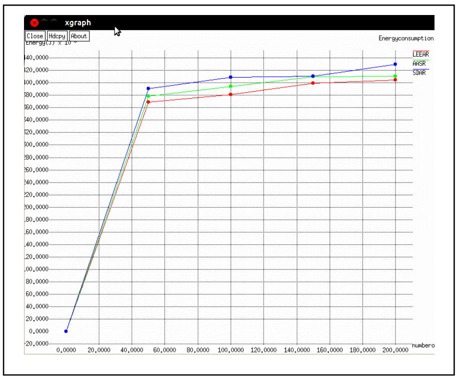
Energy consumption is reduced during generation and validation of keys. It uses anonymous private key, shared session keys and anonymous public key. In most of the existing anonymous routing protocols such as MASK [13], SDAR more control packets are used in route discovery phase. In this proposed system, due to the absence of preprocess approach, less control packets are needs and hence less energy consumption.

V. PERFORMANCE EVALUATION

The proposed system is simulated using NS-2[14] and is compared with various anonymous on –demand routing protocols. Performance metrics used are energy consumptions, packet delivery ratio, throughput and end to end delay. Results are obtained by varying number of nodes.

In the simulation scenario an adhoc network of size 1000m x 1000m consists of 50,100,150 and 200 mobile nodes. Simulation results demonstrate the comparative performance of Light weight Energy Efficient Anonymous Routing (LEEAR), AASR and SDAR by varying number of nodes.

According to Fig 2 LEEAR energy consumption is almost 20% less when compared to AASR and SDAR. Fig 3 shows LEEAR has better packet delivery ratio compared to other two.



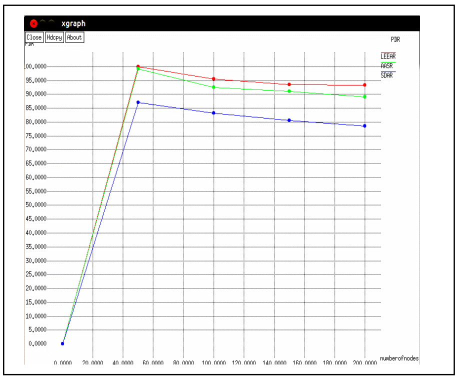


Fig 2: Energy Consumption vs Number of nodesFig 3: Packet delivery ratio vs Number of nodes

According to Fig 4 it can be inferred that the throughput of LEEAR is 20% more than the AASR and 24%more than the SDAR protocol. Fig 5 demonstrates that the end to end delay of LEEAR is better than the other two protocols.

DOI: 10.15680/IJIRCCE.2016. 0411149

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

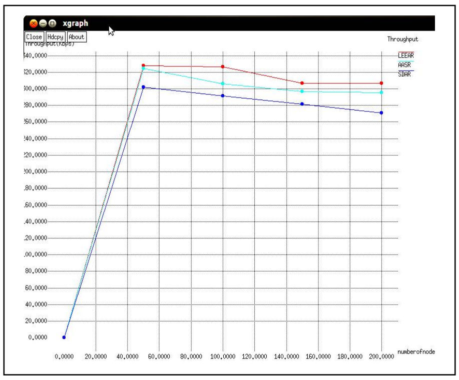


Fig 4: Throughput vs Number of nodes

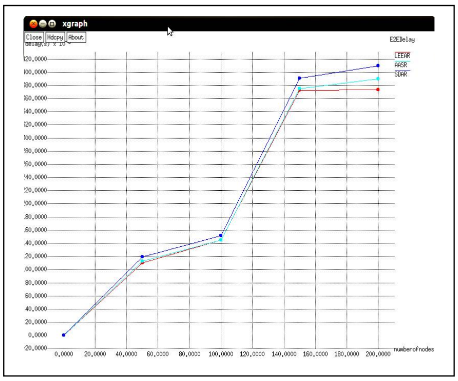


Fig 5: End to end delay vs Nodes

VI. Conclusion

Hybrid security system proposed in this paper implements an energy efficient anonymous routing protocol to achieve better security as well as energy efficiency and it is demonstrated using the simulation results. In future work, more efficient techniques can be combined to the hybrid security system to increase security & reliability.

References

1. Yanchao Zhang; Wei Liu; Wenjing Lou; "Anonymous communications in mobile ad hoc networks "INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE Volume 3, 13-17 March 2005 Page(s):1940 -1951 vol. 3
2. Jacobsson, M.; Niemegeers, I.; "Privacy and Anonymity in Personal Networks " Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on 8-12 March 2005 Page(s):130 - 135
3. F. D¨otzer, "Privacy issues in vehicular ad hoc networks," in Proc. of the Workshop on Privacy Enhancing Technologies (PET), 2005.
4. L. Abusalah, Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE Communications Surveys and Tutorials, Vol. 10, No. 4, pp. 78-93, Jan. 2008.
5. P. G. Argyroudis, and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks," IEEE Communications Surveys and Tutorials, Vol. 7, No. 3, pp. 2-21, Mar. 2005.
6. Jiejunkong and Xiaoyan Hong, "ANODR: Anonymous On Demand Routing with Untraceable Routes For Mobile Adhoc Networks," MobiHoc'03 proceedings of the 4th ACM international symposium on mobile adhoc networking & computing, pages 201-302, June 1 – 03, 2003.
7. K. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, Sep. 2011
8. Haiying Shen, Member, and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013
9. Wei Liu, Member, and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 9, NOVEMBER 2014
10. A. Boukerche, K. EI-Khatib, L. Xu, and L. Korba. "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Network", The 29th Annual IEEE International Conference on Local Computer Networks, Tampa, Florida, USA, 2004 .
11. Goldwasser,S.,S.Micali and C.Rackoff. "Knowledge Complexity of Interactive Proof Systems", Proceedings of STOC 1985, PP. 291-304
12. D. Johnson, and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Technical Report CORR 99-34, Centre for Applied Cryptographic Research (CACR), University of Waterloo, 1999.
13. Yanchao Zhang, Wei Liu and ,Wenjing Lou, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 9, SEPTEMBER 2006
14. Network Simulator: http:///www.isi.edu/nsnam/ns

BIOGRAPHY

A. Naveena is working as Assistant Professor in the department of ETM, G. Narayanamma Institute of Technology and Science, under JNTU H, Hyderabad ,Telangana. She is also pursuing PhD, under JNTU, Telangana. She received ME degree from OU, Hyderabad, Telangana, India. Her research interests are Wireless sensor networks, MANETs.

Dr. K. Ramalinga Reddy is working as Professor, HOD in the department of ETM, G. Narayanamma Institute of Technology and Science, under JNTU H, Hyderabad ,Telangana. He has completed PhD from JNTU H, Telangana. His research interests are Image Processing and Artificial Neural Networks.