Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 38 (2012) 1586 – 1591

Procedia Engineering

www.elsevier.com/locate/procedia

International Conference On Modeling Optimization and Computing

OPTIMIZING COST AND THROUHPUT EFFICIENCY WITH SECURITY IN WIRELESS AD HOC NETWORKS USING LEACH

R.Menaka[a], **N.Umamaheswari** [b,a*]

[a] *PG Student, Velammal engineering college,Chennai-66,India.*

[b] *Assistant professor, Velammal Engineering College, Chennai-66, India*

Abstract

Wireless ad hoc network (WANET) is a decentralized type of the wireless network. There are various challenges that are faced in the ad hoc environment. Wireless ad hoc networking is the enabling technology for paramount civilian and military applications requiring easy and quick (and often unmanned and cheap) network deployments. The security of communication in ad hoc wireless network is very important especially in military applications. The wireless nature of communication and any lack of network security infrastructure raise several security problems. Asymptotic notations solve the problem of large wireless networks. The main objective of the system is performance degradation of the secure network. In this paper mainly considering, order to reduce delay and increase throughput. The network performance can be calculated by using probability (p<1). Here we implemented LEACH algorithm for an efficient energy saving and thus increases the life time of wireless network. The simulation results show the presented algorithm is more efficient energy saving and fewer packets are damaged; thus provides secure wireless network.

Keywords: *wireless networks, ad hoc networks, leach*

* Corresponding author. Tel.:+91 9786915549.
E-mail address:menakarajan.2010@gmail.com.

doi:10.1016/j.proeng.2012.06.194

I.INTRODUCTION

Wireless ad hoc networks cooperate with all nodes to provide network services. Formally, a wireless ad hoc network (WANET) is a collection of autonomous nodes that communicate with each other by forming a single-hop or, often, multi-hop wireless network and by maintaining connectivity in a decentralized manner.A WAHN can be informally visualized as a group of wireless communication devices/nodes held by users coming together spontaneously to form a network for a common purpose. Due to the limited radio transmission range, data packets are usually forwarded through multiple relay nodes before they reach the destinations. Even though wireless ad hoc networks are expected to work in the any absence of fixed infrastructure, recent advances in wireless network reveal interesting solutions that enable the mobile ad hoc network nodes presents of the infrastructure. If a node always serves as a relay to transmit the packets, it may quickly use up its own energy and other resources. This is especially for wireless ad hoc networks, which offers a communication over shared wireless channel without rely on preexisting infrastructure forming a temporary network.

Security association (SA) is the establishment of shared security attributes between two network entities to support secure communication. There is a physical link between any two neighbouring nodes, and this link can be secured with the primary SA if the neighbouring nodes are also friends. We call this kind of secure link as a primary secure link. A link can also be secured with the help of other authenticated neighbours; we call this kind of secure link a derived secure link**.** Neighbouring nodes with primary SA is authenticate with each other preconfigured materials and physical link between them can be secured accordingly. Since the number and the distribution of SA's can determined by the trust relationship of embedded network of users, the probability of the node shares the primary SA's of another node.

When the population of network size n node increases the network, the physical link needs to be secure, Secure link augmentation (SLA) can be helped and performed the two friends if neighbour nodes. SLA is the procedure of securing a physical link between the two neighbouring nodes, but the nodes are not friends in this case. The need for asymptotic analysis of the network and its corresponding protocol design is useful for characterise the behaviour of network performance and its size of n grows. In the proposed methodology uses LEACH algorithm for increase the lifetime of the network.

II.RELATED WORKS

Wireless ad hoc network is a limited availability of energy with in nodes. Network life time is depends upon the system energy efficiency. Maximum life times are determining by the optimizing size and optimize the cluster head nodes [2]. [3]Clustering provides a method to build and maintain hierarchical addresses in ad hoc networks. Here, we survey several clustering algorithms, concentrating on those that are based on graph domination. In addition, show that building clustered hierarchies is affordable and that clustering algorithms can also be used to build virtual backbones to enhance network quality of service in wireless ad hoc networks. Periodic clustering based model is used for the energy consumption of wireless sensor networks and wireless ad hoc networks.

[4][10]important of throughput and delay parameters design and evaluation routing protocol ad hoc networks the throughput achieved by the algorithm is only a poly logarithmic factor off from the optimal. Analyse the performance of probabilistic algorithm. Relate the nature of the delay-capacity trade-off to the nature of the node motion, thereby providing a better understanding of the delay-capacity relationship in ad hoc networks than earlier works [10].The network is assumed to corporate routing in each other's packet, in this case each node to transmit through the power to guarantee to the network.

Critical power node transmit in the network needs to transmit in order to ensure that the network is connected with the probability one as the nodes in the network goes to infinity.

2.1.CAPACITY OF WIRELESS NETWORKS

The fundamental trade of between the achievable and delay and delay in large mobile wireless networks. The i.i.d mobility model, mobility improves the achievable capacity of static wireless networks event with constant delays [5]. [1] The capacity of wireless networks provides the two types of networks in arbitrary nodes and random nodes. There is a more challenge of theoretical information.Percolation theory: The percolation theory background that is needed to show the existence of a cluster of nodes forming the highway system An achievable bit rate per source–destination pair in a wireless network of n randomly located nodes is determined adopting the scaling limit approach of statistical physics. It is shown that randomly scattered nodes can achieve, with high probability, the same transmission rate of arbitrarily located nodes. This contrasts with previous results suggesting that a reduced rate is the price to pay for the randomness due to the location of the nodes[4].the capacity of wireless networks of randomly located nodes has the same asymptotic behaviour as the capacity of arbitrary networks[5].

[7] The lower bounds on the capacity of ad hoc wireless networks with a large number of nodes. Throughout this constraints are assumed that all the fading coefficients are independent. [6] The fundamental trade-off between the capacity and delay for a mobile ad hoc network under the Brownian motion model. Capacity of multichannel WANETs with random(c, f) assignment [16] can be utilized to analyze the secure throughput with the key pool scheme.

2.2.KEY MANAGEMENT

[11] Security mechanisms for MANETs thus far involve the heavy use of public-key certificates. Key management is a fundamental, challenging issue in securing MANETs. This paper presents IKM, a secure, lightweight, scalable ID-based key management scheme for MANETs. [12] Sensor nodes are pre-loaded with a random subset of cryptographic keys, and then deployed. Thereafter, two neighbouring nodes can communicate securely only if they share at least one common key using asymptotic notation to solve large network. [14][12] To study the frame work of prekeydistribution scheme to propose a new key predistribution scheme improves the network resilience of threshold property. [15] Large scale sensor networks to generate the pairwise random key predistribution. Binomial distribution analyses the key path length in a hop-by-hop fashion.[18] key establishment in the sensor networks present the random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation.

Public key management is a fully self-organized key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services [18]. This approach does not deliver the trust authority in a initialization phase of wireless networks. Certificates are stored in central repositories of self organized scheme. In this public key management scheme solve the difficult problems in wireless ad hoc networks. [17] Key pool scheme is the better cryptosystem asymptotic method in wireless networks. In a new way of key management scheme using sub key pool to enlarge the size of key pool. With the more keys in the key pool, this scheme has higher security against node capture. The analysis shows that this scheme provides better security compared to the previous approaches, and can ensure reasonable connectivity at the same time. Random selection nodes are easily secure with networks.

III.PROPOSED SCHEME

For maintaining security in WANET, we have to consider issues like low energy, low secure state, low processing and radio ranges. One way to increase the number node is to manage them in a hierarchy manner; that is called as clustering. This method will increase the scalability of the wireless network. From each cluster, the scheme elects cluster-head based on the parameters such as more energy, secure and degree. Cluster-head selection will be done by using LEACH algorithm. Cluster head selection is a more efficient and well structure model, it is more suitable then the one hop and multi hop model. The proposed scheme combines data from cluster-head for implementing LEACH. The performance evaluation such as secure state, life time, and throughput will be shown by using simulation results. The performance of wireless ad hoc network is highly sensitive to changes in node-to-node communication.

LEACH algorithm selects j cluster-heads of N nodes without communication among the nodes. Each node determines a random number x between 0 & 1. Cluster-head dissipate much more energy than non cluster-heads. The energy is distributed by using LEACH (Low Energy Adaptive Clustering Hierarchy). The operation of LEACH is divided into rounds. During each round a different set of nodes are cluster-head. Each node determines a random x between 0 & 1.Every node becomes cluster-head exactly once within 1/P rounds. The basic idea of using LEACH is to increase the lifetime of the network. Use of metric depends on the application. From the probability value getting from the algorithm, the decision is made about the secure, delay, throughput, scalability and energy state. The architecture model of the proposed scheme is shown in the figure 1, is a security in WANET model.

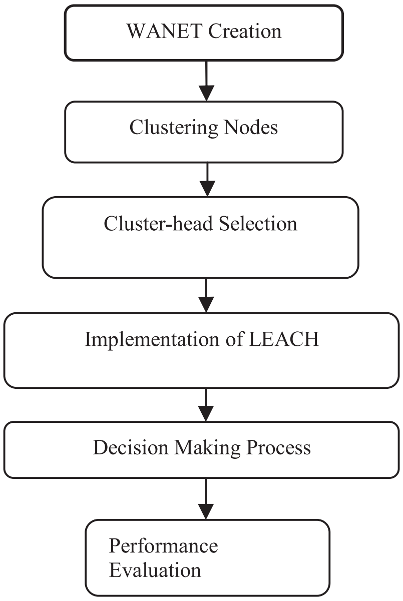

Figure 1: Security in WANET

The steps in the proposed scheme are:

Creation of WANET: We use Network Simulator to create dynamic varying topology network.

Cluster nodes: The nodes that are having small distance forms cluster. After forming cluster, we have to elect cluster-head for each cluster.

Cluster-head Selection: A wireless network consisting of a large number of nodes with limited battery power can be an effective tool for gathering data in a variety of environments. Clustering nodes into groups, so that nodes communicate information only to cluster-heads and then the cluster-heads communicate the aggregated information to the base station, may save energy. We propose an optimal energy adaptive clustering algorithm which is motivated from the LEACH protocol. We optimize LEACH's random cluster-head selection algorithm to ensure the balanced energy depletion over the whole network thus prolongs the network lifetime for wireless networks.

Implementation of LEACH: The operation of LEACH is divided into rounds. During each round a different set of nodes are cluster-head. Each node determines a random x between 0 & 1. Every node becomes cluster-head exactly once within 1/P rounds. The basic idea of using LEACH is to increase the lifetime of the network.

Decision Making Process: The decision is based on the numeric value that we get from the above step. Cluster-head observations can be used to make decision about secure, energy, scalability and throughput of the WANET.

The performance is evaluated by using decision making process. The performance of LEACH is evaluated using NS2, a simulator which is used to test and evaluate clustering algorithms.

The purposes of the simulations are:

1. To prove the unfeasibility of one hop clusters.
2. To justify our choice to limit the size of clusters.
3. To test the performance of SCA for dense networks and in different areas.
4. To compare the results such as secure, energy, delay and throughput with and without data fusion.

IV. CONCLUTION AND FUTURE WORK

A WANET can be informally visualized as a group of wireless communication devices/nodes held by users coming together spontaneously to form a network for a common purpose. In wireless ad hoc networks, all nodes cooperate to provide network services. If a node always serves as a relay to transmit the packets, it may quickly use up its own energy and other resources. The proposed scheme uses LEACH algorithm for efficient energy saving, to reduce delay, for increase throughput and secure state. In future, we may consider more nodes states such as packet delivery, secure state and energy spent to make decision about the performance degradation in WAHN. The simulation results will show the effectiveness of the proposed scheme.

REFERENCES

[1] P. Gupta and P. R. Kumar 2000. The capacity of wireless networks. IEEE Trans. Inf. Theory. (46), n, pp. 388–404.

[2]Carla Fabiana Chiasserini, ImrichChlamtac, Paolo Monti, and Antonio Nucci 2002.Energy Efficient Design of wireless ad-hoc network in Second International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols;Performance of Computer and Communication Networks; and Mobile and Wireless Communications, pp. 376-386.

[3]Arthur L. Liestman, And Jiangchuan Liu Yuanzhu Peter Chen.Clustering Algorithms For Ad Hoc Wireless Networks.

[4] M. Franceschetti, O. Dousse, D. Tse, and P. Thira 2007.Closing the gap in the capacity of wireless networks via percolation theory, IEEE Trans. Inf. Theory.(53), pp. 1009–1018.

[5] N. Bansal and Z. Liu 2003.Capacity, delay and mobility in wireless ad hoc networks. in Proc. IEEE INFOCOM, San Francisco, CA.(2), pp. 1553–1563.

[6] X. Lin and N. B. Shroff.2004. The fundamental capacity-delay tradeoff in large mobile ad hoc networks presented at the 3rd Annu Mediterr Ad Hoc NetWorkshop Bodrum, Turkey.

[7] X. Lin, G. Sharma, R. Mazumdar, and N. Shroff.2006. Degenerate delay-capacity trade-offs in ad hoc networks with brownian mobility,"IEEE/ACM Trans. Netwoks., (52). pp. 2777–2784.

[8] S.Toumpis and A. Goldsmith.2004.Large wireless networks under fading, mobility, and delay constraints in Proc. IEEE INFOCOM, Hong Kong, China.vol. (1). pp. 609–619.

[9] A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah.2006.Optimal throughput-delay scaling in wireless networks—Part II: Constant-size packets IEEE Trans. Inf. Theory, (52). pp. 5111–5116.

[10] G. Sharma, R. R. Mazumdar, and N. B. Shroff.2006.Delay and capacity trade-offs in mobile ad hoc networks: A global perspective in Proc. IEEE INFOCOM, Barcelona, Spain. pp. 1–12.

[11] Y. Zhang, W. Liu, W. Lou, and Y. Fang.2006.Securing mobile ad hoc networks with certificate less public keys IEEE Trans. Depend. Secure Comput. (3), no. 4, pp. 386–399.

[12] V. Bhandari and N.Vaidya.2008.Secure capacity of multi-hop wireless networks with random key pre-distribution in Proc. 2nd IEEE Workshop Mission-Critical Netw., Phoenix, AZ. pp. 1–6.

[13] H. Chan, A. Perrig, and D. Song.2003.Random key predistribution schemes for sensor networks in Proc. IEEE S&P,Berkeley, CA. pp.197–213.

[14] W. Du, J. Deng, Y. S. Han, and P. K. Varshney.2003.A pairwise key predistribution scheme for wireless sensor networks in Proc. ACM CCS, Washingtion, DC.pp. 42–51.

[15] D. Huang, M. Mehta, A. van de Liefvoort, and D. Medhi.2007.Modelling pairwise key establishment for random key predistribution in large scale sensor networks.IEEE/ACM Trans. Netw. (15). pp.1204–121.

[16] V. Bhandari and N. Vaidya.2007 Capacity of multi-channel wireless networks with random assignment in Proc. ACM MobiHoc,Montreal, QC, Canada. pp. 229–238.

[17] L. Eschenauer and V. Gligor.2002.A key-management scheme for distributed sensor networks in Proc. ACM CCS,Washingtion, DC. pp. 41–47.

[18] S. Capkun, L. Buttyan, and J. Hubaux.Self-organized public-key management for mobile ad hoc networks.IEEE Trans. Mobile Comput.(2). pp. 52–64.

[19] Ying Liang, Haibin Yu.Energy.Adaptive Cluster-Head Selection for Wireless Sensor Networks.IEEE 6th international conference, pp.634-638.

[20]Carla Fabiana Chiasserini, ImrichChlamtac, Paolo Monti, and Antonio Nucci.2002.Energy Efficient Design of wireless ad-hoc network in Second International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols;Performance of Computer and Communication Networks; and Mobile and Wireless Communications. pp. 376-386.