International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Hybrid Security and Energy Aware Routing for Wireless Ad hoc Networks

S. Nagendram, K. Ramchand H Rao

Abstract: ***Wireless ad hoc networks are increased with respect to data transmission between different nodes via relay routing in real time network environment. Wireless ad hoc networks are the collection of different wireless nodes which communicate over common wireless medium. Relay configuration of particular node over relay routing is a complex task which improves the quality of service parameters based on basic standards in routing communication scenarios. Different security challenges appear in this scenario because of misbehaving nature of intermediate nodes in data transmission with respect to scalability and efficiency in wireless ad hoc network communication. So that in this paper we present and develop a Hybrid approach, which consists unital key distribution approach and dynamic source optimized routing scenario to improve scalability and efficiency for key sharing to all the nodes in wireless networks. Performance of proposed approach in terms of increasing quality of service (QOS) parameters in wireless ad hoc networks.***

Key words: Wireless ad hoc networks, Key distribution, resource optimality, overlay network routing and key management schema.

I. INTRODUCTION

Wireless ad hoc network is the combination of different nodes to forming a network with any assistance related to centralized architecture. These networks are introduced a new era in terms of network formation and can be formatted and well suited wireless environment where loss of network architecture and maintain cost effectively via data transmission[1].Based on overall network maintenance, ad hoc networks to be classified as three categories, at present, we are in third network generation[2].

In hybrid wireless network system, wireless ad hoc is the combination of heterogeneous network nodes to form temporary network systems with any maintenance of centralized server with different situations. Based on this criteria, it is necessary one wireless network host forward packets to other wireless network node either it is destination or other node in network shown in figure 1.

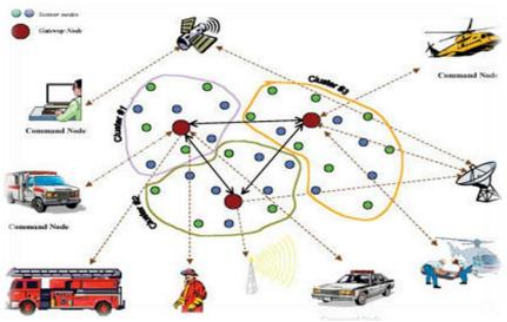

Fig .1. Network infrastructure in wireless ad hoc networks.

The above figure classifies the information in terms of different kinds of relative applications based on size and other parameter sequences in network. Privacy is the basic measure to transmit data from one to other nodes in wireless ad hoc networks. Energy maintenance is another problem to explore services in network from different nodes[3]. Main problem behind wireless ad hoc networks, energy efficiency can be addressed at different levels. Secure based energy aware is also another component in wireless ad hoc networks. On this concept, in recent years, different researchers have interested to optimize energy resource management of nodes from different locations in network demonstration with respect to data relevance and other wavelength parameters processed in wireless ad hoc networks. Different security challenges appear in this scenario because of misbehaving nature of intermediate nodes in data transmission with respect to scalability and efficiency in wireless ad hoc network communication. So that in this paper we present and develop a Hybrid approach, which consists unital key distribution approach and dynamic source optimized routing scenario to improve scalability and efficiency for key sharing to all the nodes in wireless networks. Finally our proposed approach gives better security with energy resource management for each node with equal partition of data in wireless network communication.

II. BASIC KEY MANAGEMENT DESIGN

In this section, we discuss about key management procedure which manages sending request and receiving request of each node with development of networks with limited access control with numerical properties[4]. Finally plan t (b,r,k) classified as follows Given that X be the limited set with different components, develop these parameters with family of subset of X and called them as squares of X and size k,

Revised Manuscript Received on 30 July 2019.
* Correspondence Author
S. Nagendram*, Assistant Professor, Research scholar, Department of computer science and engineering, ANU, KLEF, Guntur, AP. India.
Dr. K. Ramchand H Rao, Professor, Department of computer science and engineering, ASN College of Engineering and Technology, Tenali, Guntur, A.P, India.

each data point contain in r components at every component time t precisely generated different scenario's[5]. For example, Block design of balanced symmetric component where k=b=m2+m+1, r =k=m+1 and t=1. Representation of unitil key storage for each node in matrix V is as follows

$$\begin{pmatrix} 1 & . & . & . & . & 1 & 1 & . & . & . & 1 & . \\ . & . & . & . & . & 1 & . & 1 & 1 & 1 & . & . \\ . & . & 1 & 1 & . & . & 1 & 1 & . & . & . & . \\ 1 & . & . & 1 & 1 & . & . & . & 1 & . & . & . \\ . & . & . & . & 1 & . & 1 & . & . & 1 & . & 1 \\ . & . & 1 & . & . & . & . & . & 1 & . & 1 & 1 \\ . & 1 & 1 & . & 1 & 1 & . & . & . & . & . & . \\ 1 & 1 & . & . & . & . & . & 1 & . & . & . & 1 \\ . & 1 & . & 1 & . & . & . & . & . & 1 & 1 & . \end{pmatrix}$$

Unital description of network architecture with different comprises

$b = m_2(m_3+1)/(m+1)$ and lots of vector representation of vector $v = m_3 + 1$ concentrated on each data at each node in [2]. Each node contains m+1 data points and contained r=m_2. Each pair of different node communication concentrated on each node together with 3 designs $((m_3+1, m_2(m_3+1)/(m+1), m_2, m+1, 1))$ on the other hand $(m3+1, m+1, 1)$ at different situations for each node. Unital communication of each node by its $v \times b$ frequent network present in matrix V. In this scenario, communication each node associated with different levels in network Bj. Vector representation of classification may characterized as

$$M_{ij} = \begin{cases} 1 & \text{if } P_i \in B_j \\ 0 & \text{otherwise} \end{cases}$$

This is the basic procedure used for creating unique key for each node with simulated network parameters and describes procedure to perform efficient routing communication in wireless networks[6].

III. HYBRID APPROACH PROCEDURE FOR SECURE ENERGY CALCULATION

In this section, we describe the procedure of hybrid approach with respect to communication between nodes[7]. Also describe the procedure of energy consumption at different nodes based on whole regard of central processing units (CPU) parameters like security, trivium, and quadrivium functions and these functions[8] are iteratively perform different operations like sending receiving and others which are described as follows:

$$E_{option} = T * V * I$$

Where O_{ption} is the initial representation of CPU, option is the is the light range of what we present in time T with lots of data communication between nodes, I be the band width representation at each node and V be the Volts used in communication[9]. Dash board representation of different nodes with abnormal behavior of different nodes at different communication as follows:

$$E_H = E_{H_{CPU}} + E_{H_{COMM}}$$

Energy utilization for machinery completion with different operations like sent, receive and route communication[10]. We calculate energy consumption for each node based on heart beat rate of CPU to process nodes with communication and describe different node voltages described as follows:

Input: Nodes information from N-1to n, bandwidth, initial energy and security parameters

Output: Secure aware energy results.
Initialize the communication from n=n1,n2,....,nn.

Communicate MANET sequences based on window size from 20m
Sending request with energy 14.8m, receiving packet request 12.8 mA

Listen communication between nodes 1.8 mA.
Sensor communication with sequential data transmission from sending to receiving and appear gateway communication of MANETs with consumed energy with different parameters.

Calculate the energy for different node communication store in data evaluation.

Alg .1. Procedure to evaluate energy utilization of different nodes in network communication.

Life time of node i.e NL (G,v) at each node V in network G sorted by sending data in between them described as follows:

$$nl(G,v) = \frac{E_r(v)}{E_{cpu}(v) + Ecomm(v)}$$

E(v) describes recover energy of each node in vector V, optimized energy utilization with CPU processing of V i.e. E(CPU) with lots of communication with different functions respectfully[11]. Combination of CPU operations for different nods defined as follows:

$$E_{CPU}(v) = \sum_{i \in CPU} E_i(v)$$

CPU is the set of indexes which consists all the executed operations in node communication[12]. Combine all the operations and then describe them as follows

$$E_{COMM}(v) = \sum_{i \in COMM} E_i(v)$$

COMM is the transmitted energy for different nodes with different operations like send(),recv() and listen () in communication[13]. Finally secure energy trade-off results with respect to nodes transmit data with each with respect to required response time at different situations in wireless network communication[14].

IV. IMPLEMENTATION AND PERFORMANCE EVALUATION

This section describes the implementation of proposed approach with respect to existing approaches i.e SAMA and QoPML in data transmission with unique identification between different nodes in wireless network communication[15].

For this implementation, we use NS3 for tool implementation with C++ language for construction of network architecture with communication between different nodes using the following simulation parameters.

Used parameter	Description
Nodes by distance	350m
Data rate transmission	450m
Interface by Radius	750m
Data bit rate size	2048 bytes
Size of network communication	52
Time for simulation of nodes	35-75
Nodes description	10,20,30,40,50
Connection between nodes	4,8,16,24,31, 39
Used protocol	DSR,AODV based on TCP

Table .1. Parameter description used in network communication.

Network architecture implementation with respect to nodes communication and bandwidth for each node described in figure 2

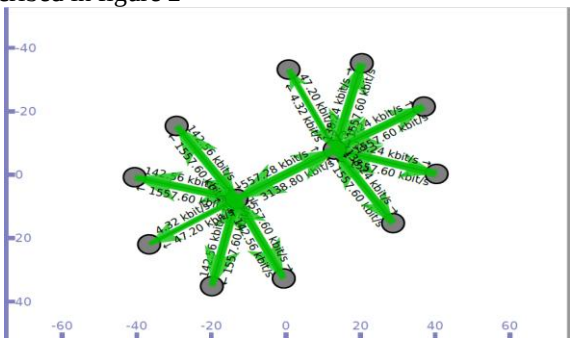

Fig .2. Network design and topology construction

. Based on above architecture for efficient communication between nodes with different bandwidth bitrates with respect to unique node communications. In this we generate randomly select number of nodes with different bandwidths at different communicative situations between nodes in network communication[16]. Basic representation of different nodes with different bandwidths shown in table 2.

Table .2. Different bandwidth values for different nodes communication in networks.

Nodes	Hybrid Approach	SAMA	QoPML
10	1.6	2.6	3.1
20	1.7	2.8	3.4
30	1.8	2.9	3.6
40	1.9	3.1	3.7
50	2	3.5	3.9
60	2.2	3.7	4.1
70	2.4	3.9	4.3

Performance of proposed approach with different bandwidth ratios for different nodes with unique secure identification in wireless network communication shown in figure 3

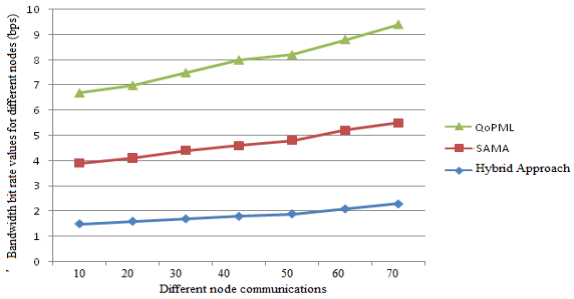

Fig .3. Performance of proposed approach with different bandwidth bit rates

Figure 3 shows the performance of hybrid approach with respect to node communication with different bit rate values communicate with each other. Based on hybrid approach procedure discussed in above section, energy utilization for different nodes communicate with other at different routing scenarios present with different bandwidths described in figure 4 with different communications in wireless networks.

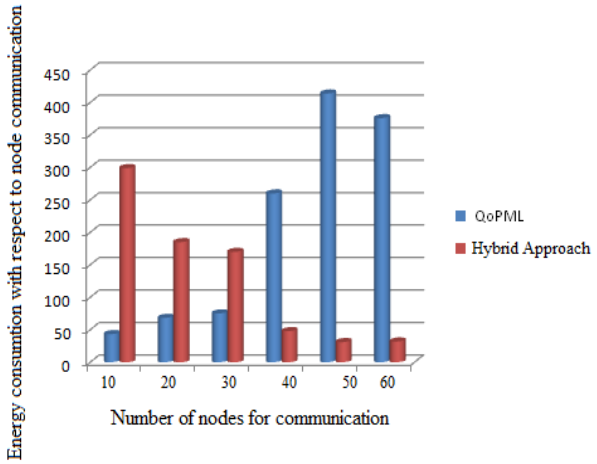

Fig .4. Performance of energy consumption with different nodes communication

Based on above results hybrid approach gives better bit rate evaluation for different nodes at energy utilization in network communication. Finally energy utilization for different nodes when compare to existing approach i.e. QoPML, proposed hybrid approach gives less utilization with different band width calculations in wireless network communication.

V. CONCLUSION

In this paper we propose a Hybrid approach which is the combination of unitil key distribution approach and dynamic and optimized source routing methodology. We describe the procedure of unitil key approach for individual nodes to generate unique for sharing data with loss in wireless communication.

Describe the procedure of dynamic and optimized routing between nodes whenever the nodes communicate with other using optimized routing scenario with less bandwidth at each node. Also measure secure aware energy utilization for data transmission at each node with updated bandwidth and energy utilization in wireless network communication. Experimental results discussed in this paper give better and efficient results with respect to privacy and energy utilization in wireless networks with comparison of existing approaches. Further improvement of this research is to extend and support optimized energy utilization with secure aware routing in wireless network communication.

REFERENCES

1. Walid Bechkit _, Yacine Challal _ and Abdelmadjid Bouabdallah, "A New Scalable Key Pre-distribution Scheme for WSN" , hal-00710086, version 1 - 20 Jun 2012.
2. An Liu and Peng Ning. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of the 7th international conference on Information processing in sensor networks, IPSN '08, pages 245–256, Washington, DC, USA, 2008. IEEE Computer Society.
3. R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk: securing sensor networks with public key technology. In In SASN 04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, pages 59–64. ACM Press, 2004.
4. Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In CHES, pages 119–132, 2004.
5. J. Zhang and V. Varadharajan. Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications, 33(2):63 – 75, 2010.
6. K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones. Security in wireless sensor networks. In Handbook of Information and Communication Security, pages 513–552. 2010.
7. D. Snchez and H. Baldus. Key management for mobile sensor networks. In Secure Mobile Ad-hoc Networks and Sensors, volume 4074 of Lecture Notes in Computer Science, pages 14–26. Springer Berlin / Heidelberg, 2006.
8. A. Ouadjaout, M. Bagaa, A. Bachir, Y. Challal, N. Lasla, and L. Khelladi. Encyclopedia on Ad Hoc and Ubiquitous Computing, chapter Information Security in Wireless Sensor Networks, pages 427–472. World Scientific, 2009.
9. L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In ACM CCS '02, pages 41–47, 2002.
10. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE SP '03, 2003.
11. W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In IEEE INFOCOM'04, pages 586–597, 2004.
12. D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In ACM CCS '03, pages 52–61, 2003.
13. R. Blom. An optimal class of symmetric key generation systems. In Proceedings of the Eurocrypt 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques., pages 335–338. Springer-Verlag, 1985.
14. Z. Yu and Y. Guan. A robust group-based key management scheme for wireless sensor networks. In Wireless Communications and Networking Conference, pages 1915–1920. IEEE, 2005.
15. Girling G., Wa J, Osborn P, Stefanova R. The Design and Implementation of a Low Power Ad Hoc Protocol Stack. *Proceedings of IEEE Wireless Communications and Networking Conference* 2000.
16. Jones CE, Sivalingam KM, Agrawal P, Chen JC. A Survey of Energy Efficient Network Protocols for Wireless Networks. *Wireless Networks* 2001; 7(4): 343-358.