International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Advanced Secure Energy Aware Trade-off Model to Control Data Communication in Wireless Networks

S. Nagendram, K. Ramchand H Rao

Abstract: ***Secure data transmission in ad hoc related wireless networks is an aggressive concept in present node to node communication. Secure energy trade-off between different node communication is also major challenge in wireless ad hoc networks. To provide efficient communication with secure data aware between nodes in ad hoc wireless networks. So that in this paper proposes and introduces Advanced Secure Energy Aware Trade-off Model (ASEATM) for energy trade results in wireless ad hoc networks, also use Elliptic curve cryptography to describe/ provide source authentication with respect to efficient communication in wireless networks. Our experimental results show efficient secure communication in wireless ad hoc networks with comparison to existing approaches in real time scenario.***

Index Terms: ***Wireless ad hoc networks, secure communication, energy consumption, elliptic curve cryptography, data transmission.***

I. INTRODUCTION

Data transmission plays out a key part in upsetting unlawful and harming data from being submitted in frameworks to spare the profitable pointer vitality in wireless ad hoc networks. Thus, numerous affirmation methods have been proposed in scholarly attempts to give message validity and unwavering quality affirmation for remote pointer frameworks these strategies can for the most part be partitioned into two classifications: open key focused systems and symmetric-key focused procedures. The symmetric-key focused methodology needs convoluted key administration, don't have of versatility, and isn't enduring to enormous quantities of hub deal strikes since the substance messaged and the beneficiary needs to talk about a master key between nodes. Master key is used as message authentication code to acquire data from one node to other node present in wireless ad hoc networks. For efficient data transmission, believe that to improve the quality of service to affirm at each node with master which is also circulated key for source authentication, which is also connected with different clients. An attacker node doesn't contain any key to access data from other node via multicast routing scenarios in real time wireless networks. To discuss about this issue, key based polynomial linear data representation is required, main idea behind this data transmission, master key is used to identify the node which is relate to same network and update the communication of each node in polynomial way.

Manuscript published on 30 September 2019.
*Correspondence Author(s)
S. Nagendram[1], 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, AP, India.

Approach used in this specification with master key relates to define communication exactly from one to other at each point in wireless networks. The propelled hubs affirm the believability of the substance through a polynomial appraisal. In any case, when the assortment of data passed on is bigger than the cutoff, the polynomial can be completely recovered and the framework is totally harmed. An elective arrangement was recommended in [6] to battle the attacker to handle communication in polynomial data evaluation. Main idea behind implementation of aggregation to factor to describe polynomial selection of nodes with efficient communication between nodes in fixed network. In any case, greater part of people uncovers that the novel aggravation can be totally removed the polynomial utilizing mistake rectifying rule procedures. So that to provide efficient communication in ad hoc networks, in this paper, propose Advanced Secure Energy Aware Trade-off Model (ASEATM) for energy trade results in wireless ad hoc networks, also use Elliptic curve cryptography to describe/ provide source authentication with respect to efficient transmission in wireless networks. Main contribution of this approach is as follows:

a) Introduce ECC in source validation based security insurance progressively remote correspondence to characterize continuous productivity. ECC methodology for Source cryptography.

b) We propose an advancement of the ASETM which enables us to acquire hazardous program investigation as a feature of strategy productivity examination.

c) Also discuss about elliptic curve cryptography to explore and access different node communication in wireless networks.

d) Experimental results describe efficient communication in networks.

II. REVIEW OF LITERATURE

Many research endeavors have been committed for creating vitality productive directing calculations. Hub's vitality is limited during dynamic correspondence as well as when they are in dormant state. Transmission power control and burden appropriation are two methodologies used to limit the dynamic correspondence vitality of individual hubs and rest/shut down mode to limit vitality of hubs during inertia. In transmission power control approach picking a high transmission power decreases the quantity of sending hubs expected to come to the required goal, yet makes over the top obstruction in a medium that is usually shared whereas,

choosing a lower transmission power decreases the impedance seen by potential transmitters yet bundles require all the more sending hubs to arrive at their required goal.

The particular objective of the heap appropriation approach [13-15] is to adjust the vitality use of every single versatile hub by choosing a course with underutilized hubs instead of choosing the most limited course [5, 6, 8]. Some exploration recommendations dependent on transmission power control are examined in [3, 4]. Stream Augmentation Routing (FAR) [9] finds the ideal steering way in a static system, for a given source–goal pair that limits the entirety of connection costs along the way. Online Max-Min Directing (OMM) [10] for remote specially appointed systems streamlines the network specification of individual nodes by amplifying the negligible remaining force, which averts the event of over-burden hubs. Power-mindful Localized Routing (PLR) [11] is a restricted, completely circulated vitality mindful steering calculation, with the supposition that a source hub has the area data of its neighbors and the goal. The fundamental objective of Minimum Energy Routing (MER) [12] isn't to give vitality proficient ways however to make the given way vitality effective by modifying the transmission control only enough to reach to the following bounce hub. The creators in [3] researches the effect of variable range power control on physical layer and system layer availability and demonstrates that variable range expands organize life time over normal range transmission.

III. ASEATM IMPLEMENTATION PROCEDURE

Main idea behind this implementation is introduced, sender sends data then receiver node describes concept of source node authenticator based on message authentication node implemented in message encrypted system on elliptic curve approach. For efficient communication in networks to describe and detect forgery associated node from all the nodes in network. In this proposed approach i.e. ASEATM use the procedure of SAMA to identify normal and abnormal nodes as well, it describe signature verification of each node without any prior knowledge to define data communication in wireless ad hoc networks

Elliptic Curve Cryptography Schema

For example p>3, related odd related primary numbers. ECC is defined as follows:

$$EC: b^2 = a^3 + ax + x \bmod p,$$

Where x,y belongs to F_p and $6x^3+27y^2 = 0 \bmod p$. Combination of set EC(F_p), consists all the points (a,b) belongs to F_p on the same curve and combine at particular node communication O, we will call it as infinity of point in curve. For sending information from source to destination, verification of generated keys in source side and destination may verified using signature generation & verification procedures in network communication, these two procedures having following steps for cryptography signature verification in communication between different nodes.

Step 1: Generate integers randomly k_A , $1 \le k_A \le N-1$

Step 2: Evaluate $r = a_A \bmod N$, where $(a_A; b_A) = k_A G$. If r = 0, return to above step 1.

Step 3: Evaluate $h_A \leftarrow h(m,r)$, h be the cryptographic hash function done in SHA-1 and describe the bit communication in left most hash

Step 6: Calculate $s = rd_A h_A + k_A \bmod N$, s = 0, return to step 2.

Step 5: (r; s) is the pair of signature, verification signature procedure having following steps in source authentication in network communication

1. Checks that $Q_A \neq O$, else it is invalid
2. check the communication curve
3. Check it's relates to QA = O

Finally generation and verification in network message communication as follows:

$$\begin{aligned}(a_1, a_2) &= sG - \mathrm{rh_A Q_A} \\ &= (rd_A h_A + k_A)G - rh_A Q_A \\ &= k_A G + rh_A Q_A - rh_A Q_A \\ &= k_A G\end{aligned}$$

Finally, represent a_1 = r signature accepts verification

Key management and control of different parameters sequences at different nodes with respect to master key and signature verification in wireless networks. All these techniques are signature node verification, based on this situation, it describes end-to-end communication using master key between different nodes, receiver verifies each node with master either this node contains secret key and it checks whether node relates to current network or not. Based on this criteria, our proposed approach gives efficient detection of DDOS and forgery related attacks with secure energy trade-off communication in wireless network systems. For Secure energy resource management in real time wireless networks the above procedure used to describe the communication between nodes in wireless ad hoc networks.

IV. EXPERIMENTAL EVALUATION

In this section, present experimental results of proposed ASEATM for secure and efficient data transmission and communication in wireless networks. To develop this application, construct network with different nodes 20-100 simulation with efficient communication, we evaluate performance of proposed approach packet delivery ratio, power consumption, network delay and other parameter in wireless network communication. Following figure describes network topology description with different bandwidth values in wireless networks.

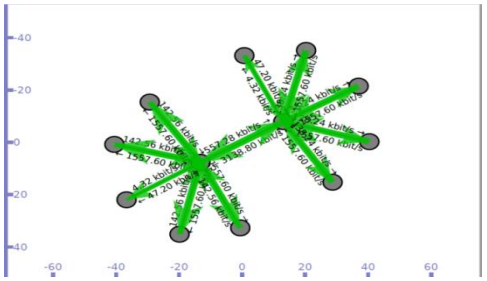

Fig 1 Network topology implementation with different node communication.

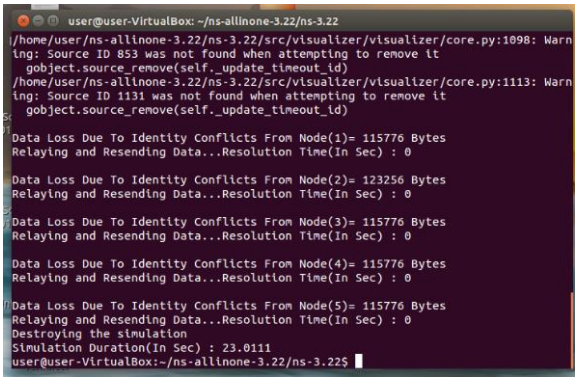

Fig 2 Real time data values for secure data communication.

Implemented results are recommended to describe situation of each node with secure energy in transmission to avoid different parameter sequences in network communication. Maintain secret key/master key for all the nodes in network, verify each network specification with secure energy consumption to enable services in wireless network communication. Time efficiency with different values is described in table 1:

Table 1 Different time values

Different nodes	ASEATM	ECC+SAMA
10	2.6	3.5
20	2.8	3.9
30	2.1	3.2
40	1.8	2.9
50	2.4	2.3
60	2.2	3.3
70	2.4	3.8

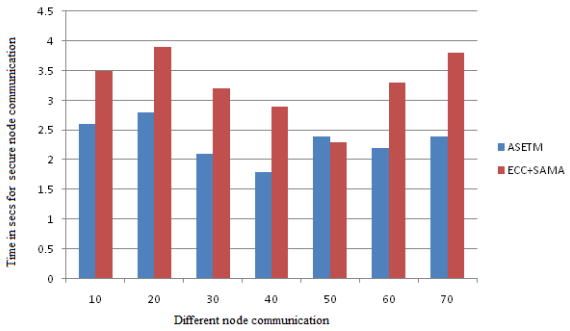

Figure 3 Performance evaluation of time values with respect to node communication.

Table 2 Secure energy trade-off communication in networks.

Nodes	ASEATM	ECC+SAMA
10	163.35	299
20	168.66	225
30	175.2	170
40	260.06	425
50	113.92	310
60	276	320

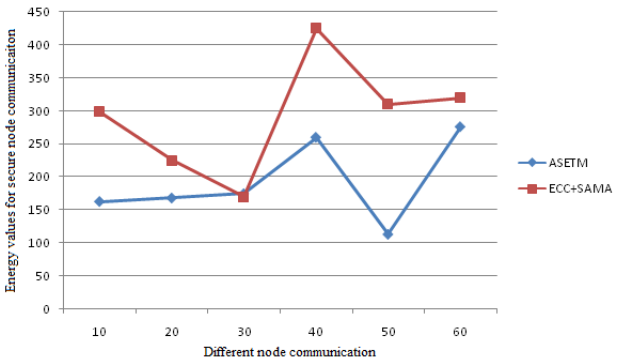

Fig 4 Performance evaluations of secure energy values.

Finally outcomes shown in figures describe performance of proposed approach with respect to energy, efficient data transmission, delivery of different packets in different node communication in wireless networks.

V. CONCLUSION

In this paper, introduce efficient (Advanced Secure Energy Trade-off Model) ASETM for energy trade results in security efforts in wireless networks. This approach used elliptic curve cryptography procedure to explore efficient communication in wireless ad hoc networks. Discuss different notation of ASETM with ECC in produce secure routing for nodes relates to different dimensions present in wireless ad hoc networks. Performance evaluation of ASETM gives better utilization in data transmission in wireless ad hoc networks with existing approaches.

REFERENCES

1. A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Boloni, D. Turgut, Routing protocols in ad hoc networks: A survey, Comput. Netw. 55 (13) (2011) 3032–3080.
2. A. D. Sarwate and A. G. Dimakis, “The impact of mobility on gossip algorithms,” IEEE Trans. Inf. Theory, vol. 58, no. 3, pp. 1731– 1742, Mar. 2012.
3. A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah, “Optimal throughput-delay scaling in wireless networks-Part I: The fluid model,” IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2568–2592, Jun. 2006.
4. A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah, “Optimal throughput-delay scaling in wireless networks-Part II: Constantsize packets,” IEEE Trans. Inf. Theory, vol. 52, no. 11, pp. 5111–5116, Nov. 2006.
5. Arati Manjeshwar and Dharma P. Agrawal,"TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks", 0-7695-0990-8/01/$10.00 (C) 2001 IEEE.
6. A. Fabrikant and C. H. Papadimitriou, “The complexity of game dynamics: BGP oscillations, sink equilibria, and beyond,” in Proc. ACMSIAM SODA, 2008, pp. 844–853.
7. A. Morton and B. Claise. (2009, Mar.). Packet delay variation applicability statement. RFC 5481 (Informational), Internet Eng. Task Force [Online]. Available: ttp://www.ietf.org/rfc/rfc5481.txt.
8. A. Nasipuri and S. Das, “Multichannel CSMA with signal powerbased channel selection for multihop wireless networks,” in Proc. 52nd Veh. Technol. Conf., 2000, vol. 1, pp. 211–218.
9. A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, “Low-cost communication for rural internet kiosks using mechanical backhaul,” in Proc. 12th Annu. ACM Int. Conf. Mobile Comput. Netw., Los Angeles, CA, USA, Sep. 2006, pp. 334–345.

10. A. Vahdatpour, F. Dabiri, M. Moazeni, and M. Sarrafzadeh, “Theoretical bound and practical analysis of connected dominating set in ad hoc and sensor networks,” in Proc. 22nd Int. Symp. Distrib. Comput., 2008, pp. 481–495
11. AbdelMoniem M-A., Mohamed H-M., Hedar A. An ant colony optimization algorithm for the mobile ad hoc network routing problem based on AODV protocol. In the proceedings of the 10th International Conference on Intelligent Systems Design and Applications, 2010.
12. András Gulyás, Gábor Rétvári, “On the Scalability of Routing With Policies”, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 23, NO. 5, OCTOBER 2015.
13. BENJIE CHEN, KYLE JAMIESON, HARI BALAKRISHNAN and ROBERT MORRIS, "Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks", Wireless Networks 8, 481–494, 2002.
14. B. Karaoglu and W. Heinzelman, “A dynamic channel allocation scheme using spectrum sensing for mobile ad hoc networks,” in Proc. IEEE Global Telecommun. Conf., 2012.
15. B. Karaoglu, and W. Heinzelman, “Multicasting vs. broadcasting: What are the trade-offs?” in Proc. IEEE Global Telecommun. Conf., Dec. 2010, pp. 1–5.
16. B. Karaoglu, T. Numanoglu, and W. Heinzelman, “Adaptation of TDMA parameters based on network conditions,” in Proc. IEEE Wireless Commun. Netw., Apr. 2009, pp. 1–9.
17. B. Karaoglu, T. Numanoglu, and W. Heinzelman, “Analytical performance of soft clustering protocols,” Ad Hoc Netw., vol. 9, no. 4, pp. 635–651, Jun. 2011.
18. B. Leiner, D. Nielson, and F. Tobagi, “Issues in packet radio network design,” Proc. IEEE, vol. 75, no. 1, pp. 6–20, Jan. 1987.
19. B. Wang, H. B. Lim, D. Ma, C. Fu. The hop count shift problem and its impacts on protocol design in wireless ad hoc networks. Telecommunication Systems, vol. 44, no. 1–2, pp. 49–60, 2010.

Retrieval Number: K22720981119/19©BEIESP
DOI: 10.35940/ijitee.K2272.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)