ISSN No: - 2456 - 2165

Enhanced Secured Data Transmission with Spatial Reusability

S.Nirmal Sam[#1], N.Rahul[*2],A.Vikas[*2]

[#]Professor,SRM Engineering College, chennai-603 203, Tamilnadu, India.

[*] Student,SRM Engineering College, chennai-603 203, Tamilnadu, India.

Abstract: **Message authentication is the process that authenticates communcaitons between two parties. Data confidentiality is the significant parameter used for measuring the ability of the system to protect the data.In the prior works , the system have two types of routing protocols, namely, single path routing and any path routing. The function of a single path routing protocols is to make wise decision for the cost minimizing path, along the packets are send from source node to destination node, but it has failed to enable the security in it.In this paper, we have proposed Spatial Reusability Aware Routing (SSAAR) with effective secure data transmission using Hop by Hop Routing algorithm. To overcome the issues in message authentication schemes,we have devoloped the technique of either symmetric-key cryptosystems or public-key cryptosystems. It includes high computational cost and several communication overhead are available in it,wchich leads to lack of scalability and resilience to node compromise attacks. We have initiated a verification model in the intermediate nodes and our model allow any node to transmit an infinite number of message without the threshold problem. The message source privacy is also designed to keep the privacy of the message during the transmission process. Experimental analysis have shown the effectiveness of the proposed work.**

Keywords: Routing, wireless network, protocol design, message authentication and data confidentiality.

I. INTRODUCTION

In the recent days,wireless Networks have attracted the researchers because of its capabilities including fault tolerance,self configuration and scalability [1]. It is a multi-hop wireless network that consists of a huge number of wireless devices , that includes mesh routers and mesh gateways. Phenomenal growth has been seen in wireless networks. The target of the wireless network is to reduce the energy usage [2].

Most of the multi-hop wireless sensor network have limited energy availability.In wireless network, reliability is the major issues of the real- time applications. Most of the applications deployed using multi-path routing systems that ensures the better reliability and service quality.The role of multipath routing is to reach its intended destination over various paths.If any link or node failure happens on the initial path, then the re-routing process is initated. Each node has to cooperate with other node to form a path and act like a relay for packet transmission. The instability of the topology link or node failures could results in disconnected routes [3].

Without any prior knowledge about the nodes, the paths are formed and the data are transmitted [4]. By sending the packets via nodes, the failure nodes can affect the network performance.Multipath scheme is used to provide energy efficient path to avoid using the interfered paths at the same time. We can choose some other links to be part of the primary path and others be the part of the protection path.The primary path and protection pathwill never transmit at the same time. Network Interference is to improve the accommodation of network connections.

In the view of wireless networks, the multipath routing intiates more than one route to process the data. Thus, the route searching is an important task in the multipath routing scheme. In some cases, node's instability and topology could leads to node's disconnection [5]. Routing in wireless networks operates based on the received requests in both dynamic and static routing.The two paths, viz, primary path and protection path are used for routing analysis. Primary path deals with failure nodes whereas protection path deals with reserved request [8].

The shared nodes could affects the network performance, if any failure node is detected. It effectively assists to save the energy.The ability ofmultipath routing schemes in providing a better QoS in transferring multimedia applications such as voice, video and data, has been proved in a number of previous studies, such as in [6]. For every received request, it performs two path for processing the data.If some network criteria are satisfied, it is possible to use a same link to protect multiple primary path.Reusability of a protection link is the ability to protect the multiple path. In wireless mesh networks,this work discuss about the reusability

ISSN No: - 2456 - 2165

[7].The received user's request is further reused for energy consumption in the networks.

The remainder of this paper is organized as in the following sections. We will describe the related works in Section 2. Section 3 will present the proposed secure spatial reusability-aware routing with enhanced secure data transmission using hop-by-hop routing algorithm. In Section 4, we will analyze the proposed method and compare it with standard reusable routing methods. Finally, a brief conclusion will be given in Section 5.

II. RELATED WORK

This section depicts the prior works carried out by other researchers.Chen et al in [10]studied about the real time video streaming process in specifi to bandwidth and energy constrained analysis. First, the single part of video is segmented into multiple parts and then transmitted to the sub-stream process.They introduced Directional Geographical Routing (DGR) which devised the load balance and the bandwidth.

Wu et al. in [11] presented a multipath routing scheme (Ad hoc on-demand multipath routing) that seeks a better quality of service in terms of bandwidth, hop count and end-to-end delay in mobile ad-hoc networks. Due to node mobility, the primary path breaks without initiating route discovery. In this case, the proposed scheme provided an alternative path to continue the data transmission. The multipath routing scheme provided QOS support with high reliability and low overloaded in simulation manner. The prior work depicted the network performance when using diverse path routing in wireless network have been studied. To improve the reliability of packets delivery by providing many alternate loop-free paths to destination , they have shown that multipath routing design.

Mohanoor et al. in [13] studied a way to improve the end-to-end throughput in wireless networks by the use of diverse paths with less interference. The author proposed a routing scheme that used multiple node-disjoint paths in indoor environments. They explored the route recovery and message control overhead. Tsai and Moors in [15] discussed multi-path routing in order to improve the end-to-end reliability. A copy of data is being send to the different paths and also the diversity in frequency are manipulated in multi-radio environment.

Similary, the author in [16] studied about the multipath routing that helps to increase the throughput rate. Another study in [17] for detecting and resolving for dynamic path deterioration in wireless networks,they presented interference-aware multi-radio routing protocol. When radical link deterioration happens,this proposed protocol dynamically reconstructs a source initiated path.Another approach for the multipath design was studied in [18].In wireless ad-hoc network, they studied the problem of finding the minimum energy disjoint paths.They have concentrated in static ad-hoc networks. They used all nodes along the primary paths named common nodes after finding a primary path in each request. To form a disjoint paths, they shared those common nodes to find a another path.

Hu and Lee in [19] proposed a multipath routing protocol named AODV-DM, that assisted to find multiple paths with less interference.An insulating region is formed around the primary path after finding a primary path.It contains all the edges in the primary path within the interference range of each node.To reduce the potential network interference with the found primary path, a protection path must be selected and established outside the insulating region.By the use of insulating region , most of the network links would be eliminated.

The author in [20] studied aboutpower delay, substantially longer network file as well as better received video quality. For better protection performance, our aim is to embrace the network interference.The interference will reduce the bandwidth of primary path, if any two of the primary path use the interfered links [21].By avoiding the use of interfered path to improve the paths bandwidth. The users cannot send or receive the large bandwidth request with the low bandwidth.In this case, they need to split the request in multiple parts.Through the multiple sends , it consumes more energy from their devices.

III. PROPOSED WORK

This section depicts the working of proposed hop by hop message authentication systems. The proposed algorithm comprised of three processes, namely, Checker Hop by Hop message authentication scheme, Signature generation algorithm and Signature verification algorithm. Let us assume a mutli-hop wireless networks with set of static N nodes. And we declared that nodes do not make use of power control scheme rather transmission rate is used. Then, the public and private keys are generated using the Elliptic Curve Algorithm. Using the generated public key and private key, the signature is designed. Atlast, the generated signature is verified which depicts verified signature can access the data packets or it gets blocked. The below fig.1 portrays the architecture of enhanced hop-by-hop message authentication systems.

3.1. Checker Hop by Hop message authentication scheme

Let p > 3 be an odd prime. An elliptic curve E is defined by an equation of the form:

$$E : y^2 = x^3 + ac + b \ mod \ p,$$

Where a, b $\in F_p$, and $4a^3 + 27b^2 \not\equiv 0 \ mod \ p$. The set E($F_p$) consists of all points (x,y) $\in F_p$on the curve, together with a special point**O**, called the point at infinity.

Let G = (x_G, y_G) be a base point on E(F_p) whose order is a very large value N. user A selects a random integer $d_A \epsilon$[1, N-1] as his private key. Then, he can compute his public key $Q_A$from $Q_A = d_A \times G$.

3.2. Signature generation algorithm:

In accord to check the message m, the computations processed by Alice is explained as follows:

1. Pick up a random integer k_A,1≤ $k_A \leq N - 1$.

2. Estimate r = $x_A mod$ N, Where $(x_A, y_A) = k_A G$. If r = 0, go back to step 1.

3. Calculate$h_A \overset{l}{\leftarrow} h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and $\overset{l}{\leftarrow}$denotes the l leftmost bits of the hash.

4. Calculate s = r$d_A h_A + k_A$mod N. If s =0, go back to step 2.

5. The signature is the pair (r,s).

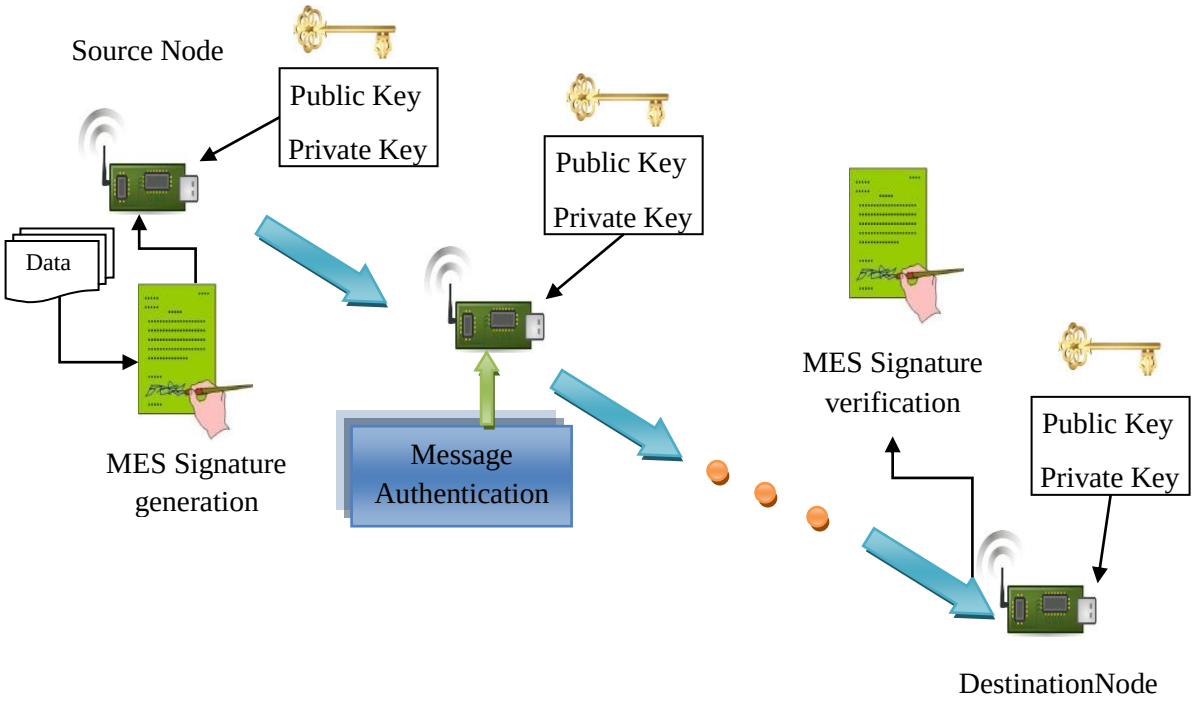

Figure 1. Proposed System Architecture

3.3. Signature verification algorithm:

The Alice's signature is further authenticated by the bob using the Alice's public key Q_A. The following processes are the signature verifications:

1. Checks that $Q_A \neq \mathbf{O}$, otherwise invalid

2. Checks that Q_A lies on the curve

3. Checks that $nQ_A = \boldsymbol{O}$

After that, Bob follows these steps to verify the signature:

1. Verify that r and s are integers in [1, N – 1]. If not, the signature is invalid.

2. Calculate $h_A \overset{l}{\leftarrow} h(m, r)$, where h is the same fucntion used in the signature generation.

3. Calculate (x_1, x_2) = sG - r$h_A Q_A$mod N.

4. The signature is valid if r = x_1 mod N, invalid otherwise.

Example:

Elliptic curve equation:

ISSN No: - 2456 - 2165

$$E : y^2 = x^3 + ac + b \bmod p$$

Let us take N=47

Let us take a=2, b=3

And Base point G= (3, 6)

It should satisfy the condition

$$4a^3 + 27b^2 \not\equiv 0$$

4x (2x2x2) +27x (3x3) =32+243

=275 $\not\equiv$ 0

The private key d_A = 31 (Random Integer from [1-46])

The public key $Q_A = d_A \times G$

Q_A =31x (3, 6)

= (93,186)

1. The random Integer k_A= 17 (Random Integer from [1-46])
2. (x_A, y_A) = 17x (3,6)

   = (51,102)

   So, x_A =51

   r =51%47

   =4
3. h_A = 12598 (Generated by SHA-1 algorithm)
4. s =4x31x12598+17%47

   = 1562169%47

   =30

   So the signature is (4, 30)

Signature verification

1. Verify r and s value
2. Calculate h_A = 12598 (Generated by SHA-1 algorithm)
3. (x_1, x_2) = 30x(3,6) -4x12598x(93,186) mod 47

   = (4, 8)
4. $r = x_1 = 4$

   So, Signature is valid.

Using the verified signature, the source node S signs its payment with their player node. Prior works depicts that receiver node validates the signature for its routing path. In view of sender node, it also checks whether the receiver node is validated or not before transmitting the data. Our proposed signature scheme ensures that the sender node can't be compromised unless the authority of receiver node is validated.

IV. EXPERIMENTAL ANALYSIS

This section depicts the experimental analysis of our proposed work. The outcomes showed that most of the received requests are responed by using two schemes. The sample cases of 500 requests are handled in 1000 * 1000 m area considered. The SSAAR routing resolved the 217 requests whereas AODV-DM protocols solved the 232 requests. Similarly, SSAAR satisfied the 42.5% dynamic requests under 1500 * 1500 m which performed better than SAAR and AODV protocols.

With the defined set of nodes, the no.of edges get decreased when the area size increases. Consider an instances 303 requests are satisfied under the area of 1000m * 1000m and 53 requests are satisfied under the area of 2500 * 2500m.The obtained results are further compared with the outcomes of SAAR and AODVDM schemes. The results depicts that AODVDM incurs high time in insulating region and the SAAR schemes works incurs high time in multi path routing systems.

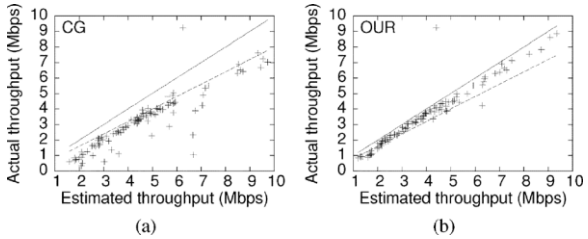

Figure 2 (a),(b). Throughput comparison

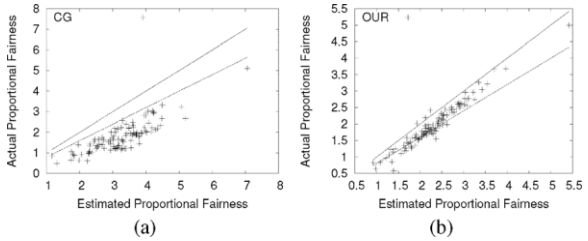

Figure 3 (a), (b). Actual versus estimated proportional fairness

ISSN No: - 2456 - 2165

From the above figures, the ratios between observed and actual throughput is analyzed. The scatterplots depicts the actual and estimated throughput using SSAAR technique.

The proposed SSAAR model satisfies more request than in SAR and AODVDM by consideringinterference and protection links reusability. It is inferred from the fig. 2 and 3, that AODV-DM can satisfy less number of requests because it hide all the edges that interfere with the primary or the protection path and it can also hide most of the links in the networks.By hiding more number of interfered edges in the graph, AODV-DM scheme will lead to a drop in the satisfied ratio and also increasing the number of nodes within the same area size.

V. CONCLUSION

To enhance secure data transmission using hop-by-hop routing algorithm, we have presented a SSAAR: secure spatial reusability-aware routing that dynamically optimizes for routing, scheduling, and simple network coding for wireless networks. A generalization of pair wise network coding and provide SSAAR, in which throughput optimal subject to the k-tuple coding constraint. For simple scenarios, we have shown achievable coding again. And it also provides simulation results for complex scenarios.For all possible scenarios,it gave an upper bond on k-tuple coding gain.Most of the benefit of k-tuple coding for the scenarios considerd of that pair- wise coding provides.

The proposed SSAARtechnique is validated via simulating the packets and evaluating the LPs with pair-wise and 3-tuple coding. The code size k increases when the topology and traffic structure of k-tuple increases. Significantly, the pair wise coding also helps to reduce the weight computingcomplexity. The similar computation model becomes signficatn in larger networks. And also the frame policy achieved better performance in 2-hop interference than the 1-hop interference.

REFERENCES

[1] A. Akella, S. Seshan, R. Karp, and S. Shenker. Selfish behavior and stability of the internet: Game-theoretic analysis of TCP. In Proceedings of the Special Interest Group on Data Communication (SIGCOMM), Pittsburgh, PA, August 2002.

[2] L. Anderegg and S. Eidenbenz. Ad hoc-VCG: a Truthful and Cost-Efficient Routing Protocol for Mobile Ad Hoc Networks With Selfish Agents. In Proceedings of the Ninth International Conference on Mobile Computing and Networking (MobiCom), San Diego, CA, Sep. 2003.

[3] N. Ben Salem, L. Buttyan, J. P. Hubaux, and M. Jakobsson. A charging and rewarding scheme for packet forwarding in multi-hop cellular networks. In Proceedings of the Fourth ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Annapolis, MD, Jun. 2003.

[4] S. Buchegger and J.-Y. Le Boudec. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing (EUROMICRO-PDP), Canary Islands, Spain, Jan. 2002.

[5] S. Buchegger and J.-Y. Le Boudec. Performance analysis of the CONFIDANT protocol (Cooperation of nodes: fairness in dynamic ad-hoc networks). In Proceedings of the Third ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Lausanne, Switzerland, Jun. 2002.

[6] L. Buttyan and J. P. Hubaux. Enforcing service availability in mobile ad-hoc WANs. In Proceedings of the First ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), Boston, Massachusetts, Aug. 2000.

[7] L. Buttyan and J. P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM Journal for Mobile Networks (MONET), special issue on Mobile Ad Hoc Networks, summer 2002.

[8] S. Eidenbenz, V. S. A. Kumar, and S. Zust. Equilibria in topology control games for ad hoc networks. In Proceedings of the 2003 Joint Workshop on Foundations of Mobile Computing, pages 2-11, 2003.

[9] S. Eidenbenz, G. Resta, and P. Santi. Commit: A sender-centric truthful and energy-efficient routing protocol for ad hoc networks with selfish nodes. In Proceedings of 5th IEEE International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (IPDPS), Apr. 2005.

[10] J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker. A BGP-based mechanism for lowest-cost routing. In Proceedings of the 21st Symposium on Principles of Distributed Computing, pages 173-182, Monterey, CA, Jul. 2002.

[11] J. Feigenbaum and S. Shenker. Distributed algorithmic mechanism design: Recent results and future directions. In Proceedings of the Sixth International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL-M), pages 1-13. ACM Press, Sep. 2002.

[12] M. Felegyhazi and J.-P. Hubaux. Wireless operators in a shared spectrum. In Proceedings of the 25th Conference on Computer Communications (INFOCOM), Barcelona, Spain, Apr. 2006.

[13] O. Goldreich. Foundations of Cryptography: Volume 1, Basic Tools. Cambridge University Press, Aug. 2001.

[14] K. Jain and V. V. Vazirani. Group strategyproofness and no subsidy via lp-duality, 2002.

[15] M. Jakobsson, J. P. Hubaux, and L. Buttyan. A micropayment scheme encouraging collaboration in multi-hop cellular networks. In Proceedings of Financial Crypto 2003, volume 2742, pages 15-33, 2003.

[16] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In Advances in Cryptology - Eurocrypt '96, volume 1070, pages 143-154, Berlin, 1996.

[17] H. Lin, M. Chatterjee, S. K. Das, and K. Basu. ARC: An integrated admission and rate control framework for CDMA data networks based on non-cooperative games. In Proceedings of the Ninth International Conference on Mobile Computing and Networking (MobiCom), pages 326-338, San Diego, CA, Sep. 2003.

[18] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the Sixth International Conference on Mobile Computing and Networking (MobiCom), Boston, MA, Aug. 2000.

[19] A. Mas-Colell, M. D. Whinston, and J. R. Green. Microeconomic Theory. Oxford Press, 1995.

[20] H. Moulin and S. Shenker. Strategyproof sharing of submodular costs: Budget balance versus efficiency. In Economic Theory, 2002.

[21] N. Nisan and A. Ronen. Algorithmic mechanism design. Games and Economic Behavior, 35:166-196, 2001.

[22] C. Papadimitriou. Algorithms, games, and the Internet. In Proceedings of the 33rd Annual Symposium on Theory of Computing, pages 749-753, Heraklion, Crete, Greece, Jul. 2001.