Privacy Preserving Data Forwarding using Multi Path Routing in Non-Cooperative Wireless Sensor Network

Adi Narayana Mogali[1], Konni Srinivasa Rao [2]

[1]*Final M.Tech Student,* [2]Asst.professor

[1,2]Dept of CSE, *Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh*

Abstract: *Today's wireless sensor network have been received much attention due to fast advancement of mobile communication. By implementing such network can be formed by numerous of heterogeneous personal mobile network. In this work, we focus on multi-path routing and forwarding in non-cooperative wireless networks, where nodes rely on each other to forward packets to the destination. Sending packets via multiple paths provide benefits such as route resilience, interference avoidance, and load/energy balancing. This paper present hybrid design for finding malicious nodes in a network, also provide for finding multi path routing and provide privacy of transferred message in the network. In this paper we are using ecliptic curve digital signature algorithm for identification of malicious or genuine nodes in a network. After finding malicious or genuine nodes we can find out multi path routing from source node to destination node. Using differentiate distance algorithm we can find out the multi path routing from source node to destination node. In this paper we can implement another concept for providing privacy of transferring message. By implementing ascii value based text data encryption process for data encryption and decryption. So that by implementing those concepts we can improve efficiency and more security of transferring message.*

Keywords: *non-cooperative networks, routing and forwarding, Security, cryptography, Multi Path Routing*

I. Introduction

Multipath Routing has long been studied as an important routing strategy in networks. It provides multiple paths for sending data from a source to a destination to exploit the resources of the underlying physical network. Previous research has demonstrated that multi-path routing can achieve route resilience, higher aggregate bandwidth, smaller end-toend delays, and better load balancing [1], [2]. Multipath routing has been explored in both wired and wireless networks. In wired network, multi-path routing is implemented as a feature of Asynchronous Transfer Mode (ATM) networks [3], Open Shortest Path First (OSPF) protocol [4], and external Border Gateway Protocol (eBGP) [5]. For wireless networks, multi-path routing is also extensively studied in recent years. A number of multi-path routing protocols for wireless networks have been proposed. Some of them [6], [7], [8], [9] maintain multiple routes and utilize these routes only when the primary root fails. Others [10], [11], [12] further schedule traffic among multiple paths in order to distribute load. In this paper, we are mainly concerned with the latter, i.e., multi-path routing protocols that assign the traffic among the multiple paths, such that transmissions can be carried out simultaneously over multiple paths. Note that while this work can actually be applied to both wired and wireless networks, we believe it has more potential impacts on wireless networks rather than on wired networks. The reason is that, in many wireless networks, devices are contributed by users, and thus the problem of selfish behavior [13], [14], [15], [16] is probably more important in the context of wireless networks than in wired networks. Therefore, we focus on wireless networks in this paper.

To ensure normal operation in non-cooperative wireless networks, it requires selfish nodes to participate in the routing protocol to establish available paths and forward packets if it is along a chosen path to a destination [17]. Since selfish nodes are mainly interested in maximizing their own payoffs, one common approach to deal with them is to design an appropriate payment mechan ism to reward cooperation. That is, if a cooperating node receives a payment more than its expended cost in forwarding a packet, then it is likely to follow the routing protocol and forward packets for other nodes. However, an important issue of this approach is to ensure that each node honestly reports its cost expenditure in forwarding a packet, otherwise, traffic sources will be asked to make unrealistic payments. In many literatures [18,19,20], mechanisms were designed for soliciting the truthful cost declaration from selfish nodesso that a certain optimal routing structure could be built to connect a source node and a destination node. The problem can be modeled as a hidden information game. In addition, another important issue is to ensure that intermediate nodes indeed forward data packets when they are asked to [21]. Unfortunately, as shown in , no dominant strategy solution exists in which every node always forwards others' packets. When packet loss occurs during forwarding, it is difficult for other nodes to distinguish whether a failure is due to natural hazard, or due to intentionally dropping by a node. Even if the protocol deploys monitoring mechanism to allow the senders or the receivers to ascertain the location of the failure, they may still be unable to attribute the causes of failure to either the deliberate action of the intermediate node, or some external factors beyond the control of the node, such as network congestion, channel interference, or data corruption. This problem is referred to as the hidden action problem.

The remainder of this paper is organized as follows. Section 2 discusses the Related work of our proposed system. Section 3 builds the mechanism and designs the algorithm that can efficiently deal with the hidden action and hidden information problem and ensure reliable multi-path routing in the link layer. Section 4 evaluates concludes this paper.

II. Related Work

Distributed algorithmic mechanism design is a recent branch of algorithmic mechanism design into the distributed computing area [22], where routing and forwarding in non-cooperative networks is an important problem of interest. A mechanism design for lowest-cost unicast routing in Internet that is built on top of BGP routing protocol was proposed by Feigenbaum et al. [23]. Feldman et al.demonstrated how an appropriate mechanism design could overcome certain hidden action problems in distributed multi-hop networks [24]. This design builds up contracts directly between endpoints and each intermediate router, as well as recursively between each intermediate router and its next hop. Such examples have demonstrated the power of combining economics concepts and cryptographic techniques with distributed routing protocols.

One common approach for handling routing misbehavior is to incentivize nodes for cooperation. Buttyan et al. proposed to use a per-hop payment carried in each packet called nuglets, to serve as incentives for packet forwarding. Following that, the authors proposed another form of incentives called counters to complement the design of nuglets [25]. Both schemes are limited by the requirement that a special secure hardware device is deployed at each node, and thus cannot be easily extended to more general networks. Zhong et al. proposed a credit-based system that does not require tamper-proof hardware at each node for credit maintenance [26]. Anderegg et al. proposed ad hoc-VCG auction to calculate proper payment for packet forwarding [27]. Combining VCG with a cryptographic technique, Zhong et al. proposed an incentive-compatible solution that corresponds to a relaxation of a dominant-action solution [29]. The VCG mechanism was also used for multi-path routing [28], [29]. With the strengths such as strategy proof ness and ex-post efficiency, VCG suffers from the overpayment problem [30], [31]. Wang et al. proposed the OURS [32] protocol for unicast routing systems. Instead of relying on a variant of VCG mechanism, OURS is built based on the concept of Nash equilibria.

III. Proposed System

A Wireless sensor network (WSN) is a system of network comprised of spatially dispersed devices using wireless sensor nodes to examine environmental or physical conditions, such as temperature, sound and movement. The individual nodes are competent of sensing their environments, processing the information statistics in the vicinity, and sending data to one or more compilation points in a WSN. Efficient transmission of data is one of the most significant issues for WSNs. Usually many WSNs are installed in unobserved, harsh and often adversarial physical environments for specific applications, such as armed forces domains and sensing tasks with unreliable surroundings. Efficient and secure transmission of data is thus very essential and is required in many such realistic WSNs. Another concept in a wireless sensor network is finding routing of transferring message. Before finding routing of message we can also perform the identification of malicious nodes or genuine nodes in a network. Those concepts can be implemented by proposed system. In this paper we are using elliptic curve digital signature algorithm for identifying malicious nodes or genuine nodes in a wireless sensor network. After finding genuine nodes in a network the server will find the multi routing path for transferring message. After finding multi routing path the server will send least cost communication path to both source node and destination node in the network. The source node will get the path and encrypt transferring message by using ascii values based data text encryption process. After completion of encryption process the source node will sent cipher format data to destination node. The destination node will retrieve the cipher format data and perform the decryption process of ascii value based data text decryption process will get the original plain format. The implementation procedure of each concept is as follows.

Initialization of nodes:

In this module each node will send request for communication process between server and client nodes in the wireless sensor network. After sending request the server will accepts request and generate ids of each client node in the network. The server will send those ids to specified client nodes in the network. Before sending ids to individual clients the server will generate distance of each node in the network. After that the server will send ids (U_i) and distance (D_i) to specified client nodes in the wireless sensor network.

Elliptic curve digital signature algorithm:

In this module each node will retrieve id and distance from the server in a wireless sensor network. After retrieving those values each client will generate signature and send those signature to server. The implementation process of elliptic curve digital signature algorithm is as follows.

Key Pair Generation Using ECDSA

Each client node will performs the following steps to generate a public and private key:

1.Select an elliptic curve E defined over a finite field F_p such that the number of points in $E(F_p)$ is divisible by a large prime n.

2.Select a base point, P, of order n such that $P \in E(F_p)$

3.Select a unique and unpredictable integer, d, in the interval $[1, n\text{-}1]$

4.Compute $Q = dP$

5.Each client private key is d

6.Each client public key is the combination (E, P, n, Q)

Signature Generation Using ECDSA

Using each clients private key, the client node generates the signature using the following steps:

1.Select a unique and unpredictable integer k in the interval $[1,n\text{-}1]$

2.Compute $kP = (x_1,y_1)$, where x_1 is an integer

3.Compute $r = x_1 \bmod n$; If $r = 0$, then go to step 1

3.Compute $h = H(U_I)$, where H is the Secure Hash Algorithm (SHA-1)

4.Compute $s = k^{-1}\{h + dr\} \bmod n$; If $s = 0$, then go to step1

5.The signature of each client is the integer pair (r,s)

Signature Verification Using ECDSA

The server can verify the authenticity of each client signature (r,s) for performing the following:

1.Obtain signatory each client public key (E, P, n, Q)

2.Verify that values r and s are in the interval $[1,n\text{-}1]$

3.Compute $w = s^{-1} \bmod p$

4.Compute $h = H(U_i)$, where H is the same secure hash algorithm used by A

5.Compute $u_1 = hw \bmod n$

6.Compute $u_2 = rw \bmod n$

7.Compute $u_1P + u_2Q = (x_0,y_0)$

8.Compute $v = x_0 \bmod n$

9.The signature each client is verified only if $v = r$

After performing verification process the server will send status to all client nodes in a network. The client will get authentication process and source node will chose destination node. The source node will send the destination id to sever and server will retrieve source, destination ids. By using those ids we can find out multi path routing by using following procedure.

Differentiate distance algorithm:

The server will get all distance of each node in the network and find out multi routing path from source node to destination node. The server will calculate all way of distance from source node to destination. After that the server will find out smallest distance from source node to destination node. By using following steps we can find out multi paths and also find out smallest routing path in all paths.

```
    $Dif_1 = D_1 - D_2$
    $Dif_2 = D_1 - D_3$ and so on
   Min=0;
 If (min< $dif_i$)
   {
      Min=$dif_i$
    Path=$U_i$
  }
```

After that we can calculate smallest distance from source node to destination node. The server will send that path to source node and destination node in the network. The source and destination node will retrieve path and sent message to destination node by using that path. Before transferring message the source node will perform the encryption for converting plain format information into cipher format. The encryption and decryption process of ascii value based data text encryption process is as follows.

Encryption process:

Step I : Input the plain text and store it.

Step II: Find the ASCII values for each characters of the input.

Step III : Find the minimum ASCII value from the data.

Step IV: Perform the modulus operation on each ASCII content value with the minimum value find in the step no. III . i.e. (ASCII Content % minimum value) If the value of mod content is greater than 16 then again perform modcontent %16 and record the positions where the value of mod content is greater than 16.

Step V: Generate a random key of 4 characters by the system.

Step VI : Find the ASCII values of the key generated.

Step VII :Find the minimum value from the ASCII values of step VI.

Step VIII : Perform the modulus operation on key ASCII values with the minimum value obtained in step VII.

Step IX : Right shift the key one time.

Step X : Add minimum ASCII value from step III to mod key values to obtain the final key.

Step XI : Add mod contents of data to the final key obtained in step X.

Step XII : Generate the cipher text from the ASCII values obtained from step XI

After getting cipher format data the source node will sent cipher data to specified destination node in the network. The destination node will get cipher format data and perform the decryption process is as follows.

Decryption Process:

Step I : Input the cipher text and find min cipher.

Step II: Obtained the ASCII values of this cipher text and find min cipher.

Step III: Find the ASCII values of final key.

Step IV : Find the minimum value of final key.

Step V: calculate the difference of ASCII values of cipher text and ASCII values of final key and add 16 To the stored positions where the mod content value is greater then 16.

Step VI : Add the min chiper to the difference to obtain the plaintext ASCII values.

Step VII: Generate the text with the help of ASCII values

By getting ascii values those ascii values can be converted into character format and get original plain format data. So that by implementing those concepts we can improve more efficiency of network and also provide more privacy of transferring message.

IV.Conclusions

In this paper we are proposed a hybrid design for providing more efficiency of wireless sensor network and also provide privacy of transferring message. Before transferring message in the network the server will perform authentication process of client nodes in the network. In this paper we are using elliptic curve digital signature algorithm for identification of malicious or genuine node in the network. After finding that the server will send status to all client nodes in the network. The server will also calculate multi routing path from source node to destination node. After finding multi routing path the server will calculate shortest path that path will be send to both node of source node and destination node. After that the source node will send the data by using that path. Before transferring message to destination node the source node will convert plain format data to cipher format by using ascii value based data text encryption process. After converting the source node will send cipher data to destination node and the destination node will retrieve cipher format data. the destination node will perform the decryption process of ascii value based data text decryption process we can get original plain format data. by implementing those concept we can improve efficiency and privacy of transferring message in a wireless network.

V.References

[1]. I. Cidon, R. Rom, and Y. Shavitt, “Analysis of multi-path routing,” IEEE/ACM Trans. Networking, vol. 7, no. 6, pp. 885–896, 1999

[2]. H. Suzuki and F. A. Tobagi, “Fat bandwidth reservation scheme with multi-link and multi-path routing in atm networks,” in Proc. IEEE INFOCOM ’92, May 1992.

[3]. CORPORATE The ATM Forum, ATM user-network interface specification (version 3.0).

[4]. J. Moy, OSPF (version 2), RFC 2328, 1998.

[5]. Y. Rekhter, T. Li, and S. Hares, "A border gateway protocol 4 (BGP-4)," RFC 4271, 2006.

[6]S.-J. Lee and M. Gerla, "AODV-BR: backup routing in ad hoc networks," in Proc. IEEE Wireless Communications and Networking Conference (WCNC '00), Sep. 2000.

[7]. M. Marina and S. Das, "On-demand multi path distance vector routing in ad hoc networks," in Proc. 9th International Conference on Network Protocols (ICNP '01), Nov. 2001.

[8]. V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in Proc. IEEE INFOCOM '97, Apr. 1997.

[9]. Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in Proc. IEEE INFOCOM '03, Mar. 2003.

[10]. S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in Proc. IEEE International Conference on Communications (ICC '01), 2001.

[11]. P. Papadimitratos, Z. Haas, and E. Sirer, "Path-set selection in mobile ad hoc networks," in Proc. Third ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '02), June 2002

[12]. M. R. Pearlman, Z. J. Haas, P. Sholander, and S. S. Tabrizi, "On the impact of alternate path routing for load balancing in mobile ad hoc networks," in Proc. 1st ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '00), Aug. 2000

[13]. L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: a truthful and costefficient routing protocol for mobile ad hoc networks with seltsh agents," in Proc. Ninth International Conference on Mobile Computing and Networking (MobiCom '03), San Diego, CA, Sep. 2003

[14]. V. Srinivasan, P. Nuggehalli, C.-F. Chiasserini, and R. Rao, "Cooperation in wireless ad hoc networks," in Proc. IEEE INFOCOM '03, Mar. 2003

[15]. W. Wang, S. Eidenbenz, Y. Wang, and X. Y. Li, "OURS: optimal unicast routing systems in non-cooperative wireless networks," in Proc. Twelfth International Conference on Mobile Computing and Networking (Mobicom '06), Sep. 2006.

[16]. S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang, "On designing incentivecompatible routing and forwarding protocols in wireless ad-hoc networks," in Proc. Eleventh International Conference on Mobile Computing and Networking (Mobicom '05), Aug. 2005.

[17]. S. Zhong, L. Li, Y. Liu, and Y. Yang, "On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: an integrated approach using game theoretic and cryptographic techniques", Wireless Networks, Vol. 13, No. 6, 2007, pp. 799–816.

[18]. J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker, "A BGP-based mechanism for lowest-cost routing", Proceedings of the twenty-first annual symposium on Principles of distributed computing, 2002, pp. 173–182.

[19]. W. Wang and X.-Y. Li, "Low-cost routing in selfish and rational wireless ad hoc networks", IEEE Transactions on Mobile Computing, Vol. 5, May 2006, pp. 596–607.

[20] W. Wang, X.-Y. Li, and X. Chu, "Nash equilibria and dominant strategies in routing", Proceedings of the First international conference on Internet and Network Economics, WINE'05, 2005, pp. 979– 988.

[21] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks", Proceedings of theINFOCOM 2003, 2003, pp. 1987–1997.

[22]. J. Feigenbaum and S. Shenker, ''Distributed Algorithmic Mechanism Design: Recent Results and Future Directions,'' in Proc. 6th Int'lWorkshop Discr. Algorithms Methods Mobile Comput. Commun., 2002, pp. 1-13.

[23]. J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker, ''A BGP-Based Mechanism for Lowest-Cost Routing,'' Distrib. Comput., vol. 18, no. 1, pp. 61-72, July 2005.

[24]. M. Feldman, J. Chuang, I. Stoica, and S. Shenker, ''Hidden-Action in Multi-Hop Routing,'' in Proc. 6th ACM Conf. Electron. Commerce, 2005, pp. 117-126.

[25]. L. Buttya´n and J. Hubaux, ''Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks,'' Mobile Netw. Appl., vol. 8,
no. 5, pp. 579-592, Oct. 2003.

[26] S. Zhong, J. Chen, and Y. Yang, ''Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks,'' in Proc. IEEE INFOCOM, 2003, pp. 1987-1997.

[27] L. Anderegg and S. Eidenbenz, ''Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad Hoc Networks with Selfish Agents,'' in Proc. MobiCom, 2003, pp. 245-259.

[28]. S. Zhong, L. Li, Y. Liu, and Y. Yang, ''On Designing Incentive- Compatible Routing and Forwarding Protocols in Wireless Ad- Hoc Networks: An Integrated Approach Using Game Theoretic and Cryptographic Techniques,'' Wireless Netw., vol. 13, no. 6, pp. 799-816, Dec. 2007.

[29]. Y. Wang, V.C. Giruka, and M. Singhal, ''Truthful Multipath Routing for Ad Hoc Networks With Selfish Nodes,'' J. Parallel Distrib. Comput., vol. 68, no. 6, pp. 778-789, June 2008.

[30] F. Wu, S. Zhong, and J. Liu, ''Cost-Effective Traffic Assignment for Multipath Routing in Selfish Networks,'' in Proc. IEEE GLOBECOM, 2007, pp. 453-457.

[31] D. Karger and E. Nikolova, ''On the Expected VCG Overpayment in Large Networks,'' in Proc. 45th IEEE Conf. Decision Control, Dec. 2006, pp. 2831-2836.

[32] K. Talwar, ''The Price of Truth: Frugality in Truthful Mechanisms,'' in Proc. 20th Annu. Symp. Theor. Aspects Comput. Sci., 2003, pp. 608-619.

[33]. W. Wang, S. Eidenbenz, Y. Wang, and X.-Y. Li, ''OURS: Optimal Unicast Routing Systems in Non-Cooperative Wireless Networks,'' in Proc. MobiCom, 2006, pp. 402-413.

BIOGRAPHIES:

Adi Narayana Mogali is student in M.Tech(CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.Tech (IT) Sarada Institute of Science Technology and Management, Srikakulam. His interesting areas are network security and web techonologis

Konni SrinivasaRao is working as an Assistant Professor in Sarada Institute of Science, Technology and Management, Srikakulam, Andhra Pradesh. He received his M.Tech (cse) from Pragati engineering college,Kakinada, East Godavari,Andhra Pradesh. His research areas include Network Security and Computer Networks