Lightweight Trust Aggregation Through Lightweight Vibrations for Trust Accumulation in Resource Constraint Mobile Ad Hoc Networks (MANETs)

Adarsh Kumar[1] , Krishna Gopal[2]
[1]Computer Science and Engineering, [2]Jaypee Institute of Information Technology
Noida, Uttarpardesh/201301, India
[1]adarsh.kumar@jiit.ac.in, [2]krishna.gopal@jiit.ac.in
www.jiit.ac.in

Alok Aggarwal
JP Institute of Engineering and Technology
Meerut, Uttarpardesh/250002, India
director@jpiet.com
www.jpiet.com

Abstract

Evaluating the trust of participating entities increases the security and collaboration among members. This work presents the trust accumulation schemes using lightweight vibration signals. In all scenarios virtual nodes are considered to create subgroup in close vicinity. It is observed that trust accumulation at virtual programmed node reduces the overhead and increases the performance of network. Lightweight vibration signals are created to accumulate trust. These signals help to find the shortest path. The system is evaluated against malicious vibrations or nodes through various attacks. Results from automated tools shows that the system is secure to be integrated.

Keywords: Ad hoc network, trust aggregation, propagation, prediction and evaluation, lightweight primitives, security.

1. Introduction

MANETs are resource constraint wireless sensor based network and require lightweight primitives to implement its services. It requires lightweight primitives in terms of computing, performance, storage, communication, security etc. Lightweight security primitives include availability, confidentiality, integrity, authentication, authorization, key management and non-repudiation [1]. In order to authenticate a particular node, trust must be established. This trust management includes: trust computation, trust propagation, trust aggregation, trust prediction and trust applications [2]. During trust propagation in local or global vicinity, trust is accumulated at subgroup member or subgroup controller through multi-paths. In order to fetch most relevant trust value, trust accumulation methods need to be integrated. These trust accumulation methods includes: sequential aggregation, conditional sequential aggregation, parallel aggregation and parallel loop aggregation [3][4]. These trust aggregations are required to be taken care at local and global level.

In this work methods to accumulate trust through vibrations are designed and analyzed. Three methods of trust accumulation are proposed. Firstly, trust is accumulated at subgroup controller. Secondly, trust is accumulated at some central subgroup member. Thirdly, trust is accumulated at some virtual node close to local subgroup boundary and nearest to subgroup to which value of trust is to be passed.

The rest of the paper is organized as follows. Section 2 presents the background work to trust management. Section 3 presents the premises and definitions used in this work. In section 4, a lightweight vibration based trust aggregation method with handling of duplicate packets is proposed. Simulation results are shown in section 5, followed by the conclusion in section 6.

2. Background

Trust management can be classified as: trust computation, aggregation, propagation, prediction and applications [10]. Trust aggregation through multipaths can remove duplicate trust score through selection of proper routes. These routes can be distinguished based on nodes or links [11][12]. Node based routes will not have common nodes among any route, whereas link based routes may have common routes but every link from source to destination will be unique. Handling of data through multipaths is extensively worked for sensor based networks [11]-[15]. In some literature these trust values are assigned based on their past experiences [16]-[17], rating mechanisms [18], reactive calculation [19] etc. In this work, idea of positive score and score for trust evaluation is extended for lightweight devices [20].

3. Assumptions and Premises

3.1. *Premises*

Let $SM_{(j,k)}^{HL_i}$ be the j^th subgroup member of k^th subgroup at i^th hierarchical layer. A set of subgroup members form subgroup $SGP_l^{HL_i}$=$\sum_{j=1}^{n} SM_{(j,k)}^{HL_i}$, Here, n is assumed to be fixed. Generally, it is kept as 10. Every $SGP_l^{HL_i}$ will have a subgroup controller $SG_l^{HL_i}$ and an identification mark $SGPIM_l^{HL_i}$. Selection of this $SG_l^{HL_i}$ is based on HEALTH i.e. HH^{MN_i}. Let T_{MN_i}be the trust of i^th mobile node. $st_i^{(x_1,y_1)}$ determine the state of a particular mobile node. P_{PATH} represents the probability of selecting a particular path. $VN_{(j,k)}^{HL_i}$ denotes the j^th virtual node in k^th subgroup at i^th hierarchical layer.

3.2. *Definitions*

Definition (Vibrations ($VIB^{SM_{(j,k)}^{HL_i}}$) ϵ {positive ($VIB_+^{SM_{(j,k)}^{HL_i}}$) or negative ($VIB_-^{SM_{(j,k)}^{HL_i}}$)}):- are the responses coming from other nodes to establish trust for sharing secret data. More positive vibrations ($VIB_+^{SM_{(j,k)}^{HL_i}}$) means high probability of sharing the secret information.

Definition (HEALTH i.e. HH^{MN_i}) [5]: of a particular mobile node (MN_i) is computed from it's energy state (ES^{MN_i}), router acting strength (RAS^{MN_i}) and positive vibration value ($VIB_+^{SM_{(j,k)}^{HL_i}}$). i.e.

$$HH^{MN_i} \epsilon \{ ES^{MN_i}, RAS^{MN_i}, VIB_+^{SM_{(j,k)}^{HL_i}})$$

Definition (Pure Soul i.e PS^{MN_i}): of MN_i is the sensor node in it's original form i.e. without be attacked.

4. Proposed Methodology

Protocol 1: Trust accumulation at CENTRE point for MN_i from intermediate nodes. Here, MN_i is more than one hop apart from CENTRE.

Step 1: In a subgroup, every node will assume itself as PS^{MN_i} and start transmitting $VIB_+^{SM_{(j,k)}^{HL_i}}$towards all directions.
Step 2: These vibrations will be received by nodes close to vicinity.
Step 3: In acknowledgement, every node will send it's subgroup identification mark ($SGPIM_l^{HL_i}$) to others. Those nodes that are in same subgroup will share trust score (T_{MN_i}).
Step 4: Those are having same $SGPIM_l^{HL_i}$ will find a center node using ((x-h)^2 /b^2 + (y-k)^2/a^2)=1. Here, (h,k) is the center point and (a,b) are (semimajor, semiminor) axis.
Step 5: Once center of gravity is found, the trust is passed to it for subgroup to subgroup communication.

Method of accumulating the trust scores at some center points overhead the network nodes to find the center point. $SG_l^{HL_i}$ is a built in entity inside a subgroup. Thus, this controller can help to transmit the trust directly to next layer's subgroup controller. This method is explained as follows:

Protocol 2: Trust accumulation at $SG_l^{HL_i}$ for MN_i from intermediate nodes. Here, MN_i is more than one hop apart from $SG_l^{HL_i}$.
Step 1:- $SG_l^{HL_i}$is assumed to be the entity with highest trust score.
Step2:- This subgroup controller will accumulate trust for subgroup members.
Step 3:- $SG_l^{HL_i}$ will determine the relevant subgroup member and it's movement.
Step 4:- At regular intervals trust values of one subgroup controller $SG_j^{HL_i}$ need to be passed to another $SG_j^{HL_{i+1}}$, These values are passed through most relevant subgroup member or subgroup controller. Subgroup member is decided based on movement of it. Markov chain will help to determine the hidden states to determine the movement. This movement is calculated as:
P($st_1^{(x_1,y_1)}, st_1^{(x_2,y_2)}$….. $st_n^{(x_n,y_n)}$) = $st_1^{(x_1,y_1)}, st_1^{(x_2,y_2)}$….. $st_n^{(x_n,y_n)}$ = P($st_1^{(x_1,y_1)} = st_1^{(x_1,y_1)}$)$p_{x_1x_2}p_{x_2x_3}$ …..$p_{x_{n-1}x_n}$=P$_{\text{PATH.}}$

Step 5:- Since subgroup controller is familiar with states of every subgroup member. This controller will decide the sensor node to transmit trust score.

Although this method of accumulating trust at subgroup controller reduces the overhead of finding the centre point to accumulate the trust but subgroup controller is another lightweight entity. It is assigned with key management, subgroup formation etc. Thus, in order to further reduce the overhead, $VN_{(j,k)}^{HL_i}$ are added and assigned the responsibility of transmitting trust.

Protocol 1: Trust accumulation at virtual node $VN_{(j,k)}^{HL_i}$ for MN_i from intermediate nodes.

Step 1:- $VN_{(j,k)}^{HL_i}$ will assume themselves as PS^{VN_i}.

Step 2:- These PS^{VN_i} will be considered as high energy programmed nodes.

Step 3:- $VN_{(j,k)}^{HL_i}$will transmit trust score to next layer $VN_{(j,k)}^{HL_{i+1}}$. This transmission could be through virtual node subgroup controller ($VNSG_{(j,k)}^{HL_i}$) to virtual node subgroup controller ($VNSG_{(j,k)}^{HL_{i+1}}$).

Step 4:- If multiple subgroup controller are having same energy level then virtual node subgroup controller is selected as:

$VNSG_{(j,k)}^{HL_i}$= MAX(HH^{VN_1}, HH^{MN_2}........HH^{MN_n})

i.e. one having the maximum health score.

Comparison: Figure 1 and figure 2 shows the performance comparison of three proposed techniques. It can be clearly seen that adding virtual nodes increases the performance of network as compared to other methods.

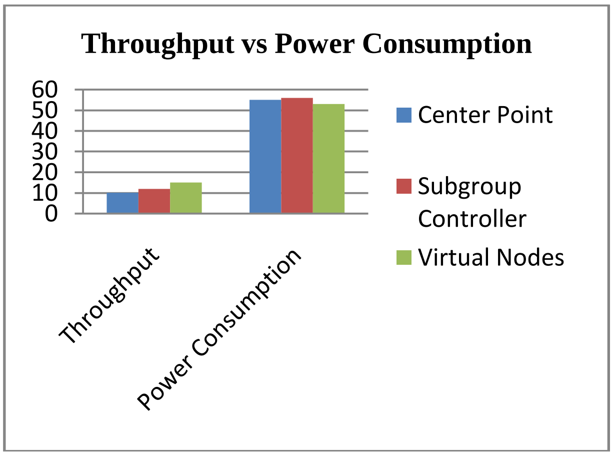

Figure 1: Throughput vs Power Consumption

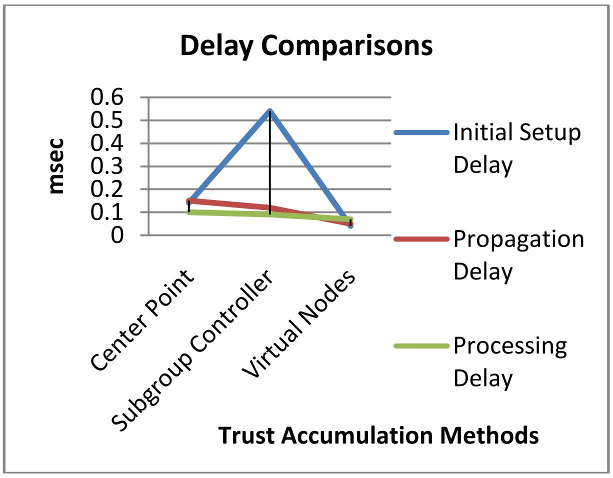

Figure 2: Delay Comparison of Proposed Techniques

From the results, it can be clearly observed that work can be easily extended with insertion of virtual nodes. Now, If a particular node want to communicate trust to $VNSG_{(j,k)}^{HL_i}$ then shortest distance between two sensor nodes is calculated. Shortest distance between two sensor nodes is calculated using Received Signal Strength Indicator (RSSI) and results into some empirical formulas[6]-[8]:

$$CL_d = CL_1 + 10 \times CAC \log d + GRV \qquad \text{(i)}$$

$$CL_1 = 10 \log G_t \, G_r ((VoL/freq)/4\pi)^2 \qquad \text{(ii)}$$

Here, $\boldsymbol{CL_d}$, CAC, d, GRV, VoL, freq, G_t and G_r are the channel loss, channel attenuation coefficient, distance, gaussian random variable, velocity of light, carrier frequency, transmission gain and receiving gain respectively. Also, GRV~ N(0,σ^2). Next, relation between RSSI and power can be measured through transmission power and receiving power as:

$$\boldsymbol{Power_{Receiving} = Power_{Transmission} / Distance(Transceiver\ Unit)^{\ n}} \qquad \text{(iii)}$$

$$Power_{Receiving}\ (dBm) = One_{mete\ r_{power}} - 10 \times nlog(Distance(Transceiver\ Unit)) \qquad \text{(iv)}$$

Here, 'n' is the propagation factor, $One_{mete\ r_{power}}$ is the receiving signal power when signal transmit one meter. In this work, relationship between RSSI and power are calculated from empirical formulas referred by Zhan et. al. and simulated using ns-2 platform[7][9]. The formulas are as follows:

$RSSI(d) = \quad Power_{Transmiss\ ion} - 40.2 - 10 \times 2 \times \log(d)$ d≤ $8m$ (v)

$RSSI(d) = \quad Power_{Transmission} \ - 58.5 - 10 \times 3.3 \times \log(d)$ d> $8m$ (vi)

Using equations (v) and (vi) distance between mobile ensor node and $VNSG_{(j,k)}^{HL_{i+1}}$ can be measured. Once after determining the distance, route with minimum energy consumption to propagate the trust is determined as:

Protocol: Trust accumulation to $VNSG_{(j,k)}^{HL_{i+1}}$ using lightweight $VIB_{+}^{VN_{(j,k)}^{HL_i}}$.

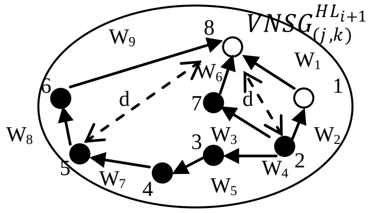

Figure 3: Trust accumulation in a subgroup.

Goal: Find the shortest path to transmit trust of $SM_{(j,k)}^{HL_i}$ to $VNSG_{(j,k)}^{HL_{i+1}}$.

Problem 1: if distance 'd' is reachable through multipath.

Step 1:- As shown in figure 3, Let suppose node 2 wants to transmit trust to node 8 then node 2 will send $VIB_{+}^{VN_{(j,k)}^{HL_i}}$. Two paths will equal number of nodes are possible to transmit trust score i.e. {2-7-8} and {2-1-8}.

Step 2:- Since node 1 is considered as PS^{MN_i}, thus route {2-1-8} is preferred.

Step 3:- If node 1 is a regular subgroup member then selection of route is dependent on weight score. These weights can be calculated using different ways. For example, interest level, signal strength, distance etc. In this work signal strength is used to calculate weight.

Problem 2: if distance 'd' is reachable through single path.

Step 1:- Suppose node 5 wants to transmit trust to node 8 then route through node 6 is the shortest path.

Step 2:- Node 5 will start transmitting its signal. It is having an option to select from {4-7-8} or {6-8}. Hence, it will prefer {6-8} path because of node disjoint, less number of nodes and less weight computation.

5. Evaluation

The proposed system is checking against various attacks using ProVerif [28]. As shown in figure 4, results show that the proposed system is protected against selected attacks.

5.1 Protection from Attacks

Attack: *Collusion Attacks*

Description: In this type of attack, attacker takes control of multiple user identification. With use of this identification, it can easily manipulate the vibration score.

Background: Dishonest feedback can be corrected using various statistical methods [21][22].

Proposed System Protection: Along with determining the health of node, the identification marks are also appended i.e. $T^i||ID^i||HTH^{MN_i}$. Since key messages are encrypted with symmetric keys. Thus, system is protected during communication.

Attack: Whitewashing and Traitor Attacks

Description: In this type of attack, when some node is continuously sending negative vibration then trust of that particular node is put on risk. In consequences, if that node wants to communicate with other nodes then it has to regain the trust.

Background: System can be protected from above attack using: acquiring a new user ID, forgetting scheme [25]-[27].

Proposed System Protection: if any node sends negative vibrations then it's trust score will automatically deteriorates. Only nodes that exceed a threshold limit are considered as reliable nodes.

Attack: Slandering attack or promoting attack

Description: Attackers fails to incorporate collusion, whitewashing and traitor attacks can insert malicious nodes to increase the vibration score. System is initialized with pure souls and these pure souls are considered to send positive vibration initially. Thereafter, Markov chain helps to determine the node's path. Thus, system can be considered as protected from above attack.

```
RESULT  not  attacker(secret SG N_SG []) is true
RESULT  not  attacker(secret SM N_SM []) is true
RESULT  not  attacker(secret SMO N_SMO []) is true
RESULT  not  attacker(secret VNSG N_VNSG []) is true
```

Figure 4: Result Evaluation using ProVerif.

5.2. Performance Analysis

In this work, python with ns-3 simulator on linux platform is used to analyze the results [9]. Figure 5 shows the comparative analysis of delays for proposed system over three MANET routing protocols i.e. Ad-hoc On-demand Distance Vector (AODV), Destination Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR). The result shows that the proposed system are having minimum delay parameters with AODV protocol.

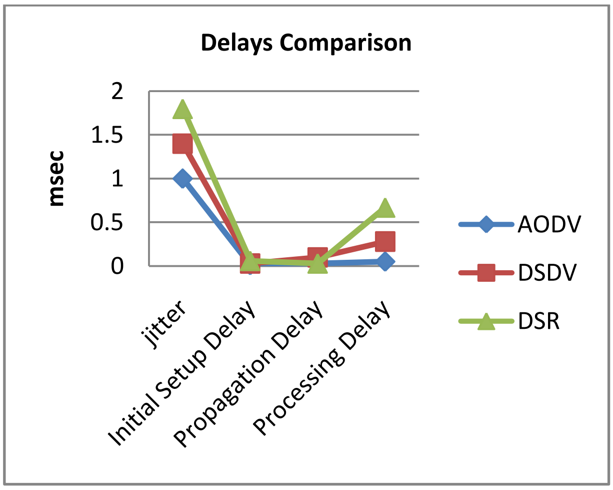

Figure 5: Delay Comparison over MANET routing protocols.

6. Conclusion

In this work, trust accumulation methods in a local subgroup are proposed for ad hoc networks. Trust accumulation at virtual subgroup controller lower the overhead caused on network as compared to trust accumulation at subgroup controller or some central subgroup member. It is also found that trust accumulation through multipaths can be aggregated based on distance. This distance is strongly related to signal strength. In order to protect the system from false vibrations or malicious entities, the system is checked against various attacks and it is seen that the system is protected from well known attacks.

References

1. L. Zhou, Z. J. Haas, "Securing Ad Hoc Networks", IEEE Network, vol. 13, no. 6, pp. 24-30, 1999.
2. Y. Sun, H. Luo, S. K. Das, "A Trust Based Framework for fault tolerant data aggregation in wireless multimedia sensor networks", IEEE Trans. Dependable Sec. Comput., vol. 9(6), pp. 785-797, 2012.
3. J. Huang and D. Nicol, "A calculus of trust and its application to PKI and identity management", in The 8th ACM Symposium on identity and Trust on the Internet, IDtrust'09, pp. 23-37, 2009.
4. K. Govindan, P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys and Tutorials, vol. 14(2), pp. 279-298, 2012.
5. Y. Sun, W. Yu, Z. Han, and K. J. Ray Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks", *IEEE JSAC special issue on security in wireless ad hoc networks*, April 2006.
6. P. Zappi, E. Farella and L. Benini, Pyroelectric InfraRed sensors based distance estimation, in IEEE Sensors 2008, (oct. 2008), pp. 716-719.
7. J. Zhan, L. X. Wu and Z. J. Tang, Research on Ranging Accuracy Based on RSSI of Wireless Sensor Network, Telecommunication Engineering, Vol. 50, No. 4, 2010, pp. 83-87.
8. Shamir A., the introduction of wireless transmission terminology, indoor propagation, path loss andexample. Electronic Products 2002:26230.
9. NS3 Simulator, http://www.nsnam.org
10. K. Govindan, P. Mohapatra, Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey, IEEE Communications Surveys and Tutorials, vol. 14(2), (2012), pp. 279-298.
11. S. Mueller, R. P. Tsang, D. Ghosal, Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges, In: Calzarossa, M. C. Gelenbe, E. (eds.) MASCOTS 2003, LNCS, vol. 2965, Springer-Heidelberg (2004), pp. 209-234.
12. S. W. Lee, J. Y. Choi, K. W. Lim, Y. B. Ko, B. H. Roh, A Reliable and Hybrid Multi-path Routing Protocol for Multi-Interface Tactical Ad Hoc Networks, In: The Military Communication Conference, (2010), pp. 1531-1536.
13. J. Zhang, C. K. Jeong, G. Y. Lee, H. J. Kim: Cluster based Multi-path Routing Algorithm for Multi-hop Wireless Network, International Journal of Future Generation Communication and Networking, (2009).
14. M. S. Siddiqui, S. O. Amin, J. H. Kim, C. S. Hong, A Secure Multi-path Hybrid Routing Protocol for Wireless Mesh Network, In: Military Communications Conference, MILCOM 2007, (Orlands FL, October 2007), p. 105.
15. M. Radi, B. Dezfouli, S. A. Razak, K. A. Bakar, LIEMRO: A Low-Interference Energy Efficient Multipath Routing Protocol for Improving QoS in Event Based Wireless Sensor Networks, In: Fourth International Conference on Sensor Technologies and Applications, SENSORCOMM, (2010), pp. 551-557.
16. D. Quercia, S. Hailes and L. Capra, B-trust: Bayesian Trust Framework for Pervasive Computing, In Proceedings of iTrust, LNCS, (2006).
17. D. Quercia, S. Hailes and L. Capra, TRULLO-local trust bootstrapping for ubiquitous devices, In Proc. Of IEEE Mobiquitous, (2007).

18. L. Page, S. Brin, R. Motwani and T. Winograd, The PageRank Citation Ranking: Bringing Order to the Web, Technical report, Standford Univeristy, (1998).
19. S. D. Kamvar, M. T. Schlosser and H. Garcia Molina, The eigentrust algorithm for reputation management in p2p networks, in Proceedings of the 12th international conference on world wide web, (2003), pp. 640-651.
20. P. Resnick and R. Zeckhauser, Trust among strategies in Internet transactions: Empirical analysis of EBay's reputation system, in Advances in Applied Microelectronics: The Economics of the Internet and E-commerce, vol. 11, In M. Baye, Ed., (Nov. 2000), pp. 127-157, Elsevier.
21. J. Weng, C. Miao and A. Goh, An entropy based approach to protecting rating systems from unfair testimonies, IEICE TRANSACTIONS on Information and Systems, vo. E89-D, no. 9 (Sep 2006), pp. 2502-2511.
22. A. Josang and R. Ismail, The beta reputation system, in Proc. Of the 15th Bled Electronic Commerce conf. (2002).
23. Y. Sun and Y. Liu, Security of Online Reputation Systems: Evolution of Attacks and Defenses,
24. K. Hoffman, D. Zage and C. Nita Rotaru, A survey of attack and defense techniques for reputation systems, technical report, Purdue Univ., (2007). http://www.cs.purdue.edu/homes/zagedj/docs/reputation survey.pdf
25. M. Abadi, M. Burrows, B. Lampson and G. Plotkin, A calculus for access control in distributed systems, ACM Transaction on Programming Languages and Systems, vol. 15, no. 4, (1993), pp. 706-734.
26. M. Feldman, C. Papadimitriois, J. Chuang and I. Stoica, Free-riding and whitewashing in peer-to-peer systems, in 3rd AnnualWorkshop on Economics and Information Security (WEIS2004), May.
27. M. Srivatsa, L. Xiong and L. Liu, Trustguard: countering vulnerabilities in reputation management for decentralized overlay networks, in Proc. Of the 14th Int. Conf. on World Wide Web, (May 2005).
28. ProVerif protocol verifier toolkit, http://www.proverif.ens.fr