Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 9; October, 2014 pp. 105-109

http://www.krishisanskriti.org/jbaer.html

Energy Aware Trust Based Routing Scheme for Mobile Ad-hoc Networks

Suyash Bhardwaj[1], Isha Bhardwaj[2], Poornima Tyagi[3]

[1]Department of Computer Science & Engineering,
Faculty of Engineering & Technology, Gurukul Kangri University, Haridwar
[2]Department of Computer Engineering, College of Technology,
GB Pant University of Agriculture & Technology, Pantnagar
[3]Department of Computer Science, Vishveshwarya Group of institutes, Greater Noida

Abstract: **In this paper we present a trust based method for providing energy aware routing in mobile ad-hoc network (MANET). This routing scheme finds the trustworthy and energy efficient secure routes for data communication. A MANET is composed of mobile nodes without any infrastructure where mobile nodes self-organize to form a network over radio links. The majority of applications of MANETs are in areas where rapid deployment and dynamic reconfiguration are necessary and wired network is not available. In such cases, it is crucial to reduce the transmission overhead and power consumption. Hence we can use Clustering in ad hoc networks; as it is useful for accomplishing scalability and robustness and it helps to save the bandwidth, thus results in reduced energy dissipation of the network. MANETs are often deployed in such places where recharge or replace of energy sources is difficult. Further, unpredicted mobility and dynamic network topology yield a serious need for battery awareness during routing. Here in this paper we used Trust-based scheme is used to assure secure end-to-end delivery of packets in the network and have explored the methods and techniques for saving battery life in MANET's.**

Keyword: **MANET, Clustering, Trust**

1. INTRODUCTION

Mobile Ad Hoc Networks are a group of self-organized, uncoordinated wireless nodes having limited energy sources and computational power [1]. They are highly deployed in battlefields, and other remote places where network set-up, replace, recharge of energy source is difficult. With ever changing topology and continuously adding and removing of nodes makes these networks highly unstable. In such situations, it is essential to devise a battery aware routing protocol to increasenetwork lifetime. The important consideration is that; in such vulnerable environment the nodes can be compromised. Once a node is compromised, the attacker can intercept any information passed through it. Theattackers can initiate denial of service (DOS) and network flooding by these compromised nodes to waste the energy of normal legitimate node[2].

Our object is to achieve the energy efficiency routing as well as reducing effect of node compromise. To evade the compromise nodes from routing, each node needs to set up local trust management on all the neighbour nodes.

In this paper we propose a trust based method to evaluate the trustworthiness of a node and to distribute the network in clusters which will be then maintained by the internal nodes based on the available battery power. The most trustworthy and energy efficient node is selected as Master Secure Node (MSN). An existing MSN makes a list of prospective MSNs and chooses one or more prospective MSNs as leader. It considers battery awareness and mobility of nodes and also ensures availability and reliability of nodes using trust-based security scheme.

2. CONCEPT OF TRUST

Trust evaluation is implemented according to normal human psychology and subsequent behaviour. In real world environments, when making decision, people normally trust the person they know personally and/or have known from someone else. They trust them till they are in a good relation with them. So how much trust a person can have on other is a relative term, if he is in communication with the person than it is supposed to be trustworthy otherwise not [3].

The MANETs are usually architecture independent networks, the work is distributed and the mutual cooperation of all nodes in the network is needed, which is based on the trust that these nodes would act as expected. However, taking each and every node to be trustworthy may not be always true, as some nodes may be compromised and behave selfishly or even maliciously to disrupt the network operation. Employing cryptographic mechanisms can protect the correctness and integrity of the information being transmitted in the system, but these mechanisms cannot answer the question about the trustworthiness of each party and predict their behaviours. By

evaluating the trustworthiness of related parties, it is easier to take proper security measures and make proper decision on any security issues[3].

3. RELATED WORK

Various papers [4,5] proposeda way to escalate the lifetime of the nodes by the use of an optimal transmission power or switching off of the nodes when they are not in active communication. In [6], a heterogeneous battery scheduling scheme has been proposed for a dual-battery-powered portable system. In [7], the authors have proposed a MAC scheduling protocol namely DWOP (distributed wireless ordering protocol) that tries to provide a fair share access of the channel for the nodes. The authors of [8] have provided an accurate model of the cell behaviour. Also, a leaky bucket traffic shaping scheme has been proposed for shaping the discharge of the batteries by modelling the traffic generated by each node. In [9], each node contains a battery pack with L cells and three battery scheduling policies have been proposedfor scheduling these L cells. In one of these schemes, whenever a packet arrives for transmission, one among the cells is chosen in a round robin fashion and discharged for providing energy to transmit the packet. Jayashree et al. have proposed energy efficient homogeneous (BAMAC) and heterogeneous (HBAMAC) battery aware MAC protocols [10], which take benefit of the chemical properties of the batteries and their characteristics, to provide fair node scheduling and increased network and node lifetime through uniform discharge of the batteries.

Extensive work has been carried out in the different aspects of proposing security models in MANETs. The work related to trust can be seen in information technology as, trust metrics and trust evaluation are mainly defined for public key authentication [11,12] access control [13] and electronic commerce[14, 15]. Ngai, Lyu and Chin [16] proposed an authentication service against dishonest nodes in MANET, by applying Beth, Borcherding and Klein's trust evaluation model designed in [17]. In Beth, Borcherding and Klein's approach, two types of trust are measured: direct trust and recommendation trust. Pirzada and McDonald [18, 19] proposed a trust model to establish trust in pure MANETs. The trust computation is based on monitoring data delivery in the network. Yan, Zhang and Virtanen [20] proposed a trust model for secure routing evaluation in MANET. The authors defined a large trust evaluation matrix based on statistic data collected during the network communication. Virendra, et al. [21] proposed a pair-wise trust evaluation scheme in MANETs. Jared Cordasco et al. [22] gave his perspective of Cryptographic Versus Trust-based Methods for MANET Routing Security. In their survey on Trust Computations and Trust Dynamics in Mobile Adhoc Networks, Kannan Govindan & Prasant Mohapatra [23] covered up various issues and challenges in the trust computation and propagation of trust in a hostile environment. Jin-Hee Cho, & Ananthram Swami [24] worked on Trust-based Cognitive Networks and gave their views on Trust Management for Mobile Ad Hoc Networks.

4. THE SCHEME

In the network scenario we assume the following properties 1) two nodes can communicate using the same transmission power level. 2) Energy usage of communicating node is more than ideal nodes 3) All nodes have similar processing capabilities and equal rights. 4) Initially all nodes are supplied with fully charged battery packs.

4.1. Node Types

There are three types of nodes in the network

1) Active Secure Node (ASN): a communicating node with Trust Certificate. Its responsibility is to keep record of its one hop neighbour and their shared trust value.

2) Ideal Sleeping Node (ISN): a node which is not in active communication. Its responsibility is to save battery so that it can be used later on.

3) Master Secure Node (MSN): a ASN node with maximum ASN as its one hop neighbours. Its responsibility is to detect malicious node and isolate them from the network; to handle trust authentication of a node; to handle leaving of a member node; to keep on updating the nearest ASN with highest Remaining Battery Power, so that in case of MSN dies a secondary MSN will take its place.

While an ASN detected as malicious, the malicious information is spread by MSN to neighbour ASNs. Therefore, malicious node cannot join to other clusters without changing its address

4.2. Shared Trust Model

We assume the trust model described in our previous work [3] for this scheme to evaluate the trustworthiness of a node.

4.2.1 Trust Quantification & Trust Computation

Trust quantification reflects various degrees of trust or distrust that a trustor node may have on a trustee node. In this paper, we express trust quantification with real number between 0 and 1. The more closure to zero represents the more degree of distrust. 1 is the maximum value that represents as absolute trust. The number 0 is a natural trust value for a new or unknown node.

In our model the trust is calculated in two types one is global trust and second is local trust. Global trust Tg is the average of addition of all local trust associated with the nodes

$$Tg = \frac{\sum_1^n Tli}{n} \quad (1)$$

and local trust Tl is the ratio of trust of Wi Weight of experience in trusted communication and Ti time for which it has been ideal.

$$Tl = \frac{Wi}{Wi+Ti} \quad (2)$$

The weight of experience is calculated as the number of successful and trusted communications of the node with other nodes. Initially when a node comes in the network after being checked through a local intrusion detection systems or some security mechanism it will be allowed in the network and hence it will get Wi as 1 at initial time. Now the local trust of the node will decrease fraction by fraction by the time Ti when it is not involved in any type of communication.

4.2.2 Making Decision

To decide that whether a node is trusted or not for current communication the difference of local trust Tl with the dynamic Tthreshold is taken into account, the decision factor D is defined as

$$D = Tl - Tthreshold \quad (3)$$

If D>=0, it means the computed trust value satisfies the trust requirement of the ongoing task. If D<0, it means that the trust requirement is not satisfied.

4.3. Battery Saving Policy

We can take the total energy utilization of a node to transmit or receive the data as the sum of energy used to transmit, receive and listen to the network. We assume that the node does not consume any considerable battery power while sleeping or in ideal state. The total consumption can be given as:

$$E = Et + Er + El \quad (4)$$

Where Et is Energy for Transmission, Er is Energy for Receiving, El is Energy for Listing.

The decision of choosing the MSN depends on the ratio of remaining battery. If the remaining battery goes below the critical point the active MSN should transfer its rights to the nearest highest powered ASN and can go to ideal state or be ASN if it is transmitting. The remaining battery level is calculated as

Battery Remaining Ratio = Used Time / Total Estimated Time ***(5)***

4.4. The Proposed Scheme for Routing

1. Neighbour management: each active node keeps track of its single-hop neighbour nodes and their remaining battery capacity of same cluster or of different clusters by exchanging periodic Hello messages. MSN maintains a member table for all its member nodes. The member table consists of the member id, remaining battery capacity by exchanging information periodically.

2. Route discovery: when a node wants to communicate with another node an algorithm is used to set up battery aware trusted route.

3. Route maintenance: route maintenance procedure is called whenever there is a link failure detected by a node on an active route. This procedure works similar to AODV with modifications as follows: when an intermediate node detects the next hop, which is missing from the route, it unicasts an RERR message to MSN. On receiving the RERR message, MSN reinitiates the route discovery procedure to establish a new route. This reduces the routing overhead as compared to AODV.

Algorithm 1 : MSN selection

For all ASN
{ Broadcast selection request message to all 1-hop neighbours
If ASN is active
{ Call algorithm 2 to check ASN trust certificate
Return (BOOL Y/N)

If ASN is trusted Node

{ Get the remaining battery power and update selection table with ASN number and remaining battery power
Battery Remaining Ratio = Used Time / Total Estimated Time
If the current MSN battery power < Critical limit
{ Choose the First ASN with highest battery remaining ratio
Set it as new MSN
Set old MSN as ASN and turn it off/ set to ideal state
}
Else
{ Broadcast message to re calculate the remaining battery power
}
}

Else
{ Set the table with distrusted ASN and update all ASN with broadcast message
}
}

Else
{ Update table with ASN ideal and update all ASN with broadcast message
}
}

Algorithm 2 : to find trusted ASN

For all ASN
{ Broadcast message for active communication time Tl request
{ find Tl $Tl = \frac{Wi}{Wi+Ti}$
find Tg $Tg = \frac{\sum_1^n Tli}{n}$
Find D $D = Tl - Tthreshold$
If D>0
{ Update table for ASN trusted
}
Else
{ Update table for ASN not trusted
}
}
}

The algorithm will work on every ASN and it will help the ASN's to keep their cluster safe and secure from the outside attacker. If an attacker tries to enter the secure cluster, it shall have to communicate to a member ASN of the cluster, which in turn will evaluate the trust level of the new coming node. In this case as the untrusted node has not yet produced any trust certificate; which was only be issued by the same cluster or the other communicating cluster. So it will be discarded immediately and the communication request will be cancelled. While in the other case if the node has the trust certificate then its trust value will be evaluated by the MSN and it will be allowed to join the network. In the due course of time if the node is compromised then it will again be moved out of the network as the algorithm checks the trust level of nodes on periodic basis. The battery power remains conserved in this secure network. If any node loses its power it goes to a hibernation state without losing its current state and data, which is then transferred to the nearest neighbour. In this way the integrity, authenticity of the network is kept.

5. CONCLUSION& FUTURE SCOPE

This paper presents energy aware trust based routing scheme for providing secure communication with least battery power usage. This scheme can be implemented on highly distributed ad-hoc networks in any kind of scenarios. In this paper we have considered battery awareness and mobility of nodes and also ensured availability and reliability of nodes using trust-based security scheme. This work contributes in making a more accurate energy model which has been proposed by incorporating important parameters for energy consumption of a node during transmission and reception of packets. Although this work has brought out some upcoming research areas as well as given a platform for the development of new routing schemes where there can be security, integrity as well as authenticity of the end to end data communication. In future more security features can be added to make the mobility of the nodes more secure and also more methods of battery saving can be implemented.

REFERENCES

[1] Nishant Gupta, Samir R. Das, Inc. "Energy-Aware On-Demand Routing for Mobile Ad Hoc Networks" OPNET Technologies, 7255 Woodmont Avenue, Bethesda, MD 20814 U.S.A.

[2] Waleed S. Alnumay, Pushpita Chatterjee & Uttam Ghosh "Energy Aware Secure Routing for Wireless Ad Hoc Networks" IETE JOURNAL OF RESEARCH, VOL 60, NO 1, JAN- FEB 2014, pp 50- 59

[3] S. Bhardwaj, S. Aggarwal and S. Goel, A Novel Technique of Securing Mobile Adhoc Networks using Shared Trust Model, International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 9 (2013), pp. 909-916

[4] S. Jayashree, B. Manoj, and C. S. R. Murthy, "On using battery state for ad hoc wireless networks," in Proceedings of ACM MOBICOM 2004, Philadelphia, PA, Sep. 2004, pp. 360-73.

[5] C. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks," IEEE Commun. Mag., Vol. 39, No. 6, 2001, pp. 138- 47.

[6] P. Rong, and M. Pedram, "Battery-aware power management based on Markovian decision processes," in Proceedings of ICCAD 2002,San Jose, CA, 2002, pp. 707-13.

[7] V. Kanodia, C. Li, A. Sabharwal, B. Sadeghi, and E. Knightly, "Ordered packet scheduling in wireless ad hoc networks: Mechanisms and performance analysis," presented at the Proceedings of ACM MOBIHOC, Lausanne, Switzerland, 2002, pp. 58-70.

[8] C. Chiasserini, and R. Rao, "A traffic control scheme to optimize the battery pulsed discharge," in Proceedings of IEEE MILCOM, Atlantic City, NJ, 1999, pp. 1419-23.

[9] C. Chiasserini, and R. Rao, "Energy efficient battery management," in Proceedings of IEEE INFOCOM 2000, Tel Aviv, Vol. 2, 2000, pp. 396-403.

[10] Jayashree, B. Manoj, and C. S. R. Murthy, "Network lifetime driven MAC protocols for ad hoc wireless networks," Springer Wireless Networks, Volume 14, no. 6, 2008, pp. 929- 47.

[11] Josang, A. An Algebra for Assessing Trust in Certification Chains. in Proceedings 1999 Network and Distributed System Security Symposium. 1999. Reston, VA, USA: Internet Society.

[12] Levien, R. and A. Aiken. Attack-resistant trust metrics for public key certification. in Proceedings of the Seventh USENIX Security Symposium. 1998. San Antonio, TX, USA: USENIX Association.

[13] Herzberg, A., Y. Mass, and J. Michaeli. Access control meets public key infrastructure, or: assigning roles to strangers. in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 2000. Berkeley, CA, USA: IEEE.

[14] Manchala, D.W. Trust Metrics, Models and Protocols for Electronic Commerce Transactions. in Proceedings. 18th International Conference on Distributed Computing Systems (Cat. No.98CB36183). 1998. Los Alamitos, CA, USA: IEEE Computer Society.

[15] Manchala, D.W., E-commerce trust metrics and models. IEEE Internet Computing, IEEE 2000. 4(n2): p. p 36-44.

[16] Nagi, E.C.H., M.R. Lyu, and R.T. Chin. An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks.

in Proceedings of 2004 IEEE Aerospace Conference. 2004. Big Sky, MT, United States: IEEE.

[17] Beth, T., M. Borcherding, and B. Klein. Valuation of Trust in Open Networks. in 3rd European Symposium on Research in Computer Security (ESORICS '94). 1994. Brighton, UK: Springer Verlag.

[18] Pirzada, A.A. and C. McDonald. Trusted Route Discovery with TORA Protocol. in the Second Annual Conference on Communication Networks and Services Research (CNSR'04). 2004. Fredericton, N.B., Canada: IEEE.

[19] Pirzada, A.A. and C. McDonald. Establishing trust in pure ad-hoc networks. in Proceedings of the 27th conference on Australasian computer science. 2004. Dunedin, New Zealand: Australian Computer Society.

[20] Yan, Z., P. Zhang, and T. Virtanen. Trust Evaluation Based Security Solution in Ad Hoc Networks. in Proceedings of the Seventh Nordic Workshop on Secure IT Systems 2003. 2003. Norway.

[21] Virendra, M., et al. Quantifying Trust in Mobile Ad-Hoc Networks. in International Con-ference on Integration of Knowledge Intensive Multi-Agent Systems, 2005 (KIMAS '05). 2005. Waltham, Massachusetts, USA: IEEE.

[22] Jared Cordasco, Susanne Wetzel, "Cryptographic Versus Trust-based Methods for MANET Routing Security" Department of Computer Science, Stevens Institute of Technology, Hoboken, New Jersey USA.

[23] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey".

[24] Jin-Hee Cho, Ananthram Swami, "Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks" Army Research Laboratory – Computer and Information Sciences Directorate, 14th ICCRTS, "C2 and Agility".