An Energy-Aware Secured Routing Protocol for Mobile Ad Hoc Networks Using Trust-Based Multipath

Isaac Woungang[1], Sanjay Kumar Dhurandher[2], and Michael Sahai[1]

[1] Department of Computer Science
Ryerson University, Toronto, Ontario, Canada
iwoungan@scs.ryerson.ca, msahai@ryerson.ca
[2] Division of Information Technology
Netaji Subhas Institute of Technology, University of Delhi, India
dhurandher@gmail.com

Abstract. Message security in multi-hop infrastructure-less networks such as Mobile Ad Hoc Networks has proven to still be a challenging task. A number of trust-based secure routing protocols have recently been introduced which comprise the traditional route discovery phase and a data transmission phase. In the later, the action of relaying the data from one mobile node to another relies on the peculiarity of the wireless transmission medium as well as the capability of source nodes to keep their energy level at an acceptable and reasonable level, posing another concern which is that of energy efficiency. This paper proposes an Energy-aware Trust Based Multi-path secured routing scheme (E-TBM) for MANETs, based on the dynamic routing protocol. Results show that our E-TBM scheme outperforms the Trust Based Multi-path (TBM) secured routing scheme - chosen as benchmark - in terms of energy consumption in the selected routing paths, and number of dead nodes, chosen as performance metrics.

1 Introduction

A mobile ad-hoc network (MANET) is a collection of highly wireless mobile nodes organized to create a temporary connection between them to forward the data, without any pre-established network infrastructure or extraneous hardware to assist in this communication. To fulfill this capacity, some form of collaborative or corporately multi-hop strategy is required to happen between the mobile nodes, which may not necessary prevail since misbehaving nodes could be part of the current set of MANET nodes. Therefore, securing the message delivery in MANETs is a key concern.

Typically, the routing mechanism involves two steps, namely the route discovery phase and the actual data transmission phase using the discovered secured route. The former relies on the underlying targeted routing protocol (in this case, we use trust-based multi-path DSR). On the other hand, the later involves investigating the peculiarities of the wireless transmission medium used as well as determining the required battery level of the source nodes involved in the data transmission process. Indeed, when performing the data transmission, it is essential that the nodes (here referred to as battery operated computing devices) that carry the operation be energy conserving

J.J. Park et al. (Eds.): GPC 2013, LNCS 7861, pp. 517–525, 2013.

so that their individual battery life can be prolonged, and the maximum lifetime of the network be achieved. These facts have led to the consideration of energy-efficiency as another important design aspect that should be taken into account in the routing decision, the goal being to achieve secure routing while lowering the network overall power consumption and number of dead nodes; where a dead node is defined as a node which has completely depleted its power level. This paper adds energy considerations into our recently proposed message security scheme in MANETs (so-called Trust Based Multi-path message security (TBM)) [1], in order to strengthen its design. Typically, the route discovery and selection algorithm in [1] is substantially modified to take into consideration the energy level of the selected routing paths while maintaining their security and trust levels, resulting to our so-called Energy-Aware Trust Based Multi-path message security protocol (so-called E-TBM). The modification consists in assigning a power-aware metric [2] to each node involved in the selected routing paths so as to quantify the amount of energy consumed by the node, thereby determine the energy consumption necessary to maintain an acceptable level of message security in the network. Our E-TBM approach consists of a combination of trust assignment mechanism, soft-encryption technique, and multi-path DSR-based routing, where the decision on the routing selection paths is energy constrained.

The rest of the paper is organized as follows. In Section 2, we present some related work. In Section 3, the proposed E-TBM approach is described in-depth. In Section 4, simulation results are presented. Finally, Section 5 concludes our work.

2 Related Work

Secured routing protocols for MANETs have been the subject of interest to the research community in the recent years. These protocols have been designed to satisfy the primary principles of network security, i.e. confidentiality, integrity, and availability, each having its own dynamics for achieving such goal. Approaches that have been proposed include: credit-based schemes; cryptographic-based methods; reputation-based schemes; methods specifically designed to protect the route discovery process; message security schemes based on trust-based multi-paths using conventional routing protocols, and others [1].

In this paper, our focus is on message security schemes based on trust-based multi-paths routing, where energy constraint is directly embedded in the design approach. Apart from relying on the proper selection of hardware, such approach must also involve the study of coupling among layers of the system since energy consumption does not occur only through transmission, but also through processing. Following this trend, representative energy-aware secured routing schemes for MANETs follows.

In [3], Sheng et al. introduced a DSR-based energy efficient routing protocol for MANETs (called NCE-DSR) which uses the number of times that a node sends messages as a parameter for deciding on the inclusion of this node in the selected routing path. A routing cost function is designed for determining the choice of the routing path. However, the overhead generated from this method is not revealed. In [4], Vadivel and Bhaskaran proposed an

energy-efficient and secured routing protocol (called Intercept detection and correction (IDC)) for MANETs. The IDC algorithm identifies the malicious nodes by recognizing the selective forwarding misbehavior from the normal channel losses by means of a residual energy parameter. However, no clue is provided as to how this energy related parameter is determined. In [5], Babu proposed an energy-based secure authenticated routing protocol (called EESARP) for MANETs. The EESARP scheme uses an attack resistant authentication combined with hop-by-hop signatures to mitigate the routing misbehavior of potential malicious nodes while improving the reliability of the route request packet. In [6], Taneja and Kush proposed an energy-efficient and authentic routing protocol (called EESSRP) for MANETs which incorporates security (by means of hash key generation and Diffie-Hellman protocol) and power features in its design. In [7], Banerjee et al. proposed a trust based multipath OLSR routing protocol for MANETs (called ESRP) where trust is established by means of a signed acknowledgement based on asymmetric key cryptography. Unlike these schemes, our proposed E-TBM scheme is a mimic of our recently TBM scheme [1], where energy consumption at each node is incorporated within the route selection phase to decide on the secure route to transfer the message.

3 The Energy-Aware Trust Based Multi-path Message Security Scheme

Assuming that a source node, say S, wishes to transmit a message, say *m,* to a destination node, say D, our E-TBM approach follows the same steps as the TBM approach [1] to securely send the message. The method consists of a combination of message encryption, message routing using DSR, and message decryption as follows.

A. Message Encryption

At node S, the message *m* is segmented into four blocks *a, b, c,* and *d* and encrypted using soft-encryption. Typically, a XOR operation on bits is used, producing the message parts *a', b'*, *c'*, and *d'* as follows [1]:

$$a' = a \text{ XOR } c,\ b' = b \text{ XOR } d,\ c' = c \text{ XOR } b, \text{ and } d' = d \text{ XOR } a \text{ XOR } b \quad (1)$$

B. Message Routing Using DSR

This step combines a trust mechanism and an enhanced DSR-based routing technique to securely transfer the encrypted parts a', b', c', and d'. The details are as follows.

Trust Mechanism: A node observes each of its neighbors to which its packets can be transferred then it assigns a discrete trust value in the range [-1, 4] to every neighbor based of the acknowledgements of the packets that it received and the trust recommendations from its peers [1]. These values are taken into account when making the decision to route the packets using DSR. When doing so, the trust defined strategy consists of the policy that a node with a certain trust assigned level *t* can be given the right to read and forward at most *t* parts of the message.

Routing Strategy: When a source node needs to route a message to a destination node, a route request (RREQ) packet is broadcasted. If a neighbor node that replies to the RREQ has the route to the destination or if the packet reaches the destination node, a route reply (RREP) is sent back to the source node acknowledging a successful delivery. In the packet header, the RREP message and trust levels of the previous nodes involved in the packet forwarding are sent backwards along the routing path selected by DSR. The current battery level (energy) of a node (computed as shown in Equation (2) – obtained from [2]) is added to the packet header:

$$Ej(t) = Ej(0) - \left(\sum_{t=0}^{Gj(t)} Cp(\tau) + CT(\tau)\right) - \left(\sum_{t=0}^{Xj(t)} (CR(\tau) + Cp(\tau))\right) - \left(\sum_{t=0}^{Rj(t)} [CR(\tau) + Cp(\tau) + CT(\tau)\right) \quad (2)$$

where *Gj(t)* is the number of packets generated by node j up to time *t; Xj(t)* is the number of packets received by node j up to time *t; Rj(t)* is the number of packets relayed by node *j* up to time *t; Cp(*$\boldsymbol{\tau}$*), CT(*$\boldsymbol{\tau}$*), and CR(*$\boldsymbol{\tau}$*)* are the processing power cost, transmitting power cost, and receiving power cost of packet $\boldsymbol{\tau}$ respectively. The E-TBM algorithm finds the secure routes from a set of given routes as follows:

1. When a new route is found, these routes are arranged in the increasing order of their hop count. Two counters are set, one to keep track of the selected nodes in the routing paths, the other to keep track of nodes energy values.
2. The first route is selected and it is assumed that the maximum number of message parts that can be routed through it have been routed. No actual routing is done at this step.
3. The next route is selected and it is assumed that the maximum number of message parts that can be routed via have been routed. If all the parts of message can be routed securely, the actual routing is done by using the selected paths.
4. If four paths have been selected out of all possible combinations of paths, arrange these paths by the energy it would be required to send the data
5. Select the path that has the smaller energy path value. Out of the remaining paths, use the next lowest path energy, and so on.
6. Repeat this process until secured routes are found.
7. If no secured routes are found, the algorithm is repeated by starting at Step 2, by selecting second route as the first route.
8. This algorithm is repeated until all the combinations of the paths are exhausted. If no secured route is found, the algorithm waits for another route. If all routes have been found or a specific time interval has expired, it is assumed that the algorithm has failed.

The above process for selecting the secured routes is captured in Fig. 1.

```
Arrange the paths P=P1, P2,..., Pn} in increasing order of path length
Initialize Count Cj for all nodes = 0
Initialize Count Ej for all nodes Energy to 0
Select the smallest path from P {
        Select the next smallest path
            if(for all selected nodes j, Cj <= Tj){
                if( four paths selected){
                  if(for all selected nodes j,
          Ej ≤ Threshold_Ej){
                            /* Th_Ei is a threshold on the battery power of the node. Ei is cal-
                            culated using Equation (2) */
                            Select path with smaller energy value
                    }
           Select next smallest path with lowest
                    energy
            else
                            continue;}
      if(all paths are exhausted)
                Wait for another path
   }
   if (no paths left)
   Print("Not possible to route securely")
```

Fig. 1. Algorithm to select secure routes

C. Message Decryption

At the destination node D, the encrypted message parts a', b', c', and d' are decrypted to recover the original message m as follows [1]:

$$a = b' \text{ XOR } d',\ b = a' \text{ XOR } b' \text{ XOR } c' \text{ XOR } d',$$
$$c = d' \text{ XOR } b' \text{ XOR } d',\ d = d' \text{ XOR } c' \text{ XOR } d' \quad (3)$$

4 Performance Evaluation

A. Simulation Tool and Parameters

To compare the E-TBM scheme against the TBM scheme, we use the GloMoSim simulation tool [10], where our soft encryption using multiple message parts is implemented at the application layer. We also assume that the trust levels of nodes are available to the source nodes. The remaining simulation setup is given in Table 1.

Table 1. Simulation parameters

Parameter	Setting
Terrain dimension	2000 m x 2000 m
Number of nodes	Variable and placed uniformly throughout the terrain dimension
MAC protocol	IEEE 802.11
Radio transmission power	Variable and depends on the number of nodes used.
Traffic Type	CBR
Simulation Time	600 s
Initial battery power of each node	5000 Joules

The following performance metrics are considered: (1) *Route selection time* – i.e. the total time required for the selection of a routing path, and (2) *trust compromise* – i.e. the sum of access violation in all the paths selected for routing. The access violation at a node n is defined as the difference between $n_{parts,}$ the number of encrypted message parts that n has received and $T_{n,}$ the trust level of n if $n_{parts} \geq T_n$, i.e. if N_p is the set of nodes in a routing path p, the trust compromise for path p is:

$$TrustCompromise_p = \Sigma_{n \in Np} (n_{parts} - T_n), \quad (4)$$

wherever $n_{parts} \geq T_n$. and T_n is the trust assigned to node n and n_{parts} is the number of encrypted message parts received by node n from all the paths. The aggregate trust compromise is calculated for all the paths selected for routing. It has been demonstrated [1] that the trust compromise of the selected paths in the T-EBM scheme is always equal to zero; (3) the *number of dead nodes:* a dead node is defined as a node which has completely depleted its power level. When a node is drained of all its available power, it no longer plays a role in the route selection process; (4) The *total energy consumed by the selected routing paths*: This is the energy consumed by the nodes that are chosen to be part of the selected routing paths.; (5) The *total energy consumed in the network*: This is the energy consumed by all the nodes in the network, regardless of their involvement in the route selection process.

B. Simulation Results

The trust compromise for the E-TBM and TBM schemes are presented in Fig. 2. As expected, regardless of the number of nodes, the total trust compromise of both schemes is equal to 0. This result is in agreement with that obtained in [1]. This is due to the fact in both schemes, the routing paths are selected according to the policy that no node in such path can receive more encrypted message parts than its trust level would permit.

Next, we compare the route selection times for the two algorithms. The results are depicted in Fig. 3. In Fig. 3, it can be observed that the route for the E-TBM scheme has increased overall compared to that of the TBM scheme. This can be attributed to the fact that in the E-TBM scheme, more computation and time are required in selecting the paths with the least amount of energy while maintaining the secure route. We also compare the total energy consumed (in Joules) by the nodes that are selected for

the secure transmission in both schemes. The results are captured in Fig. 4. In Fig. 4, it can be observed the energy consumed in the case of the TBM algorithm is significantly higher compared to that of the E-TBM algorithm. This constitutes a justification of taking the energy required to transmit a packet into account when designing secured routing protocols for MANETs.

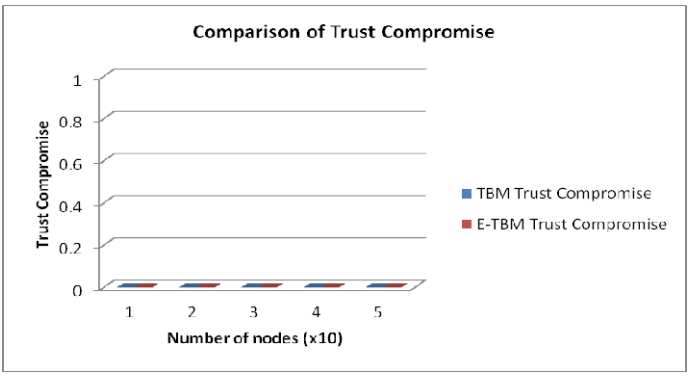

Fig. 2. Total trust compromise of E-TBM vs. TBM schemes

Next, we compare the total energy (in Joules) consumed in the network. The results are shown in Fig. 5. In Fig. 5, it can be observed that for E-TBM scheme, the overall energy consumption required for multiple paths to be selected securely and for messages to be sent down those multiple paths is much lower than that experienced with the TBM scheme.

Our simulation is started with each node having 5000 Joules of power, which decreases according to the type of routing operation being performed and which involves that node. In Fig. 6, it can be observed that by the end of the simulation, there were fewer nodes that had depleted their power (dead nodes) in the E-TBM scheme compared to the TBM scheme. This result is a direct correlation to the decreased total energy observed in the case of E-TBM. Since the total energy consumption is lower, nodes will survive longer, thus, the lifetime of the network will be increased.

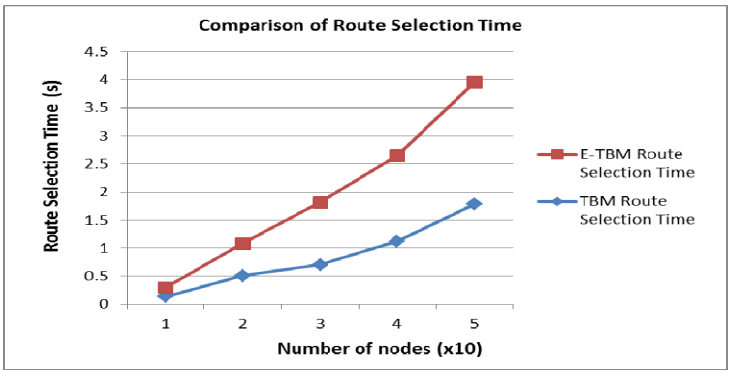

Fig. 3. Route selection time for E-TBM vs. TBM schemes

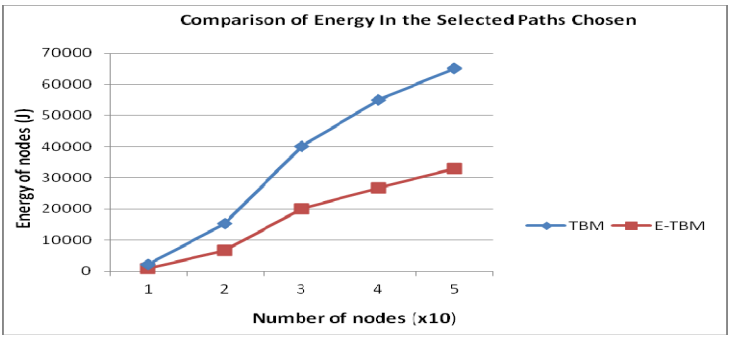

Fig. 4. Total energy consumed in the selected routing paths for E-TBM vs. TBM schemes

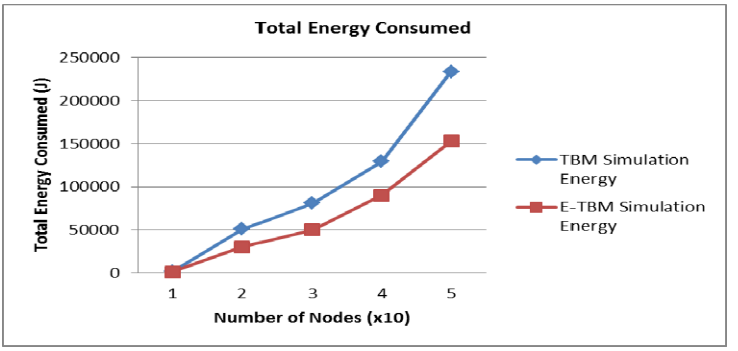

Fig. 5. Total energy consumed for E-TBM vs. TBM schemes

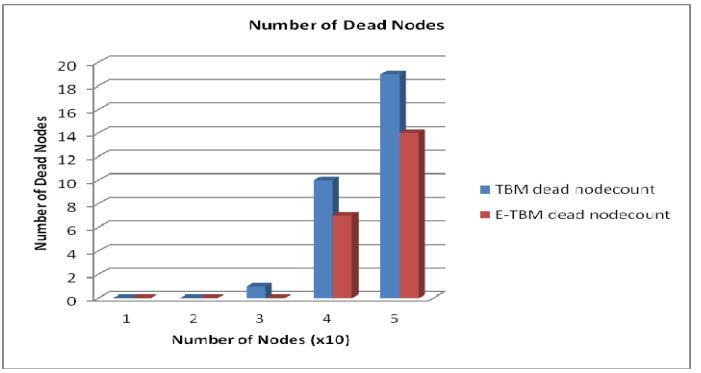

Fig. 6. Number of dead nodes in the E-TBM vs. TBM schemes

5 Conclusion

We have proposed a DSR-based secured routing scheme for MANETs and proved that it uses an energy efficient secure paths selection mechanism which minimizes the number of dead nodes, hence maximizes the network life time compared to the TBM scheme. We also observed that there is a compromise between message security (trust compromise) and routing time for both schemes. In future, we intend to compare our scheme against other known energy-aware secured routing protocols for MANETs.

References

1. Narula, P., Dhurandher, S.K., Misra, S., Woungang, I.: Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing. Computer Commuications 31(4), 760–769 (2008)
2. Roux, N., Pegon, J.-S., Subbarao, M.W.: Cost Adaptive Mechanism to Provide Network Diversity for MANET Reactive Routing Protocols. In: Proc. IEEE MILCOM (2000)
3. Singh, S., Woo, M., Raghavendra, S.: Power-aware with Routing in Mobile Ad Hoc Networks. In: Proc. of ACM/IEEE Intl. Conference on Mobile Computing and Networking (MobiCom 1998), Dallas, TX, USA (1998)
4. Vadivel, R., Bhaskaran, V.M.: Energy Efficient with Secured Reliable Routing Protocol (EESRRP) for Mobile Ad-Hoc Networks. Procedia Technology, 703–707 (2012)
5. Babu, M.R.: An Energy Efficient Secure Authenticated Routing Protocol for Mobile Adhoc Networks. American Journal of Scientific Research (9), 12–22 (2010) ISSN 1450-223X
6. Taneja, S., Kush, A.: Energy Efficient, Secure and Stable Routing Protocol for MANET. Global Journal of Computer Science and Technology, Network, Web and Security 12(10), Version 1.0 (May 2012)
7. Banerjee, A., Bhattacharyya, A., Bose, D.: Power and Trust Based Secured Routing Approach in MANET. Intl. Journal of Security, Privacy and Trust Management (IJSPTM) 1(3/4) (2012)
8. Zeng, X., Bagrodia, R., Gerla, M.: Glomosim: A library for the parallel simulation of large-scale wireless networks. In: Proc. of the 12th Workshop on Parallel and Distributed Simulation, Banff, Alberta, Canada, pp. 154–161 (May 1998)