I.J. Computer Network and Information Security, **2014, 11, 13-19**
Published Online October 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.11.02

An Improved Trusted Greedy Perimeter Stateless Routing for Wireless Sensor Networks

P. Raghu Vamsi
Department of Computer Science and Engineering, Jaypee Institute of Information Technology, Noida, India.
Email: prvonline@yahoo.co.in

Krishna Kant
Department of Computer Science and Engineering, Jaypee Institute of Information Technology, Noida, India.
Email: k.kant@jiit.ac.in

Abstract—In this paper, an improvement over Trusted Greedy Perimeter Stateless Routing (T-GPSR) is presented. T-GPSR employs heuristic weight values to evaluate total trust value of neighboring nodes. However, heuristic assignment of weights provide flexibility but it is not suitable in presence of several security attacks such as Grey hole, selfish behavior, on-off attack etc., are launched in the network in different proportions. To overcome this limitation, an improvement is suggested with an emphasis on trust update, lightweight trust computation and storage to reduce communication and storage overhead. The simulation study indicates that the packet delivery ratio of the improved T-GPSR has improved by 10% over T-GPSR in the presence of 50% of malicious nodes in the network.

Index Terms—Trust, security, geographic routing, reputation, security attacks, wireless sensor networks.

I. Introduction

Wireless Sensor Networks (WSNs) are best candidates for the applications like earth quake detection, fire in forest detection, blood pressure monitoring in health care applications, temperature and humidity monitoring, pollution monitoring in environmental applications, supply chain management, body area networks, pressure and speed monitoring in automotive, pungent gas or chemical detection in industries, target detection in military etc. [1-2]. Basically, these networks composed of inexpensive and tiny sensor nodes (SNs) with limited resource in-terms of processing, energy and memory. The task of each sensor node is to sense the environment and report the data to the destination node in a single or multi hop fashion with localized routing decisions. Numerous researchers have designed routing protocols to adapt to a variety of applications. A defacto classification provided for these routing algorithms are reactive, proactive and geographic or location aware protocols. Reactive protocols identify route based on the received route request dynamically. In contrast, proactive protocols maintain a routing table for ready availability of routes. Whereas location based routing takes place based on nodes' location information. The packets will be forwarded to the node which is in the location near to the destination with an extensive use of location information.

In case of any routing protocol, effective communication can be guaranteed only with positive cooperation among nodes. But, the limitations of sensor networks such as wireless communication, lack of tamper proof bodies, unattended deployment etc., often lead to vulnerabilities and prone to security attacks. Research studies in WSNs have shown that the packet delivery percentage can degrade substantially when malicious nodes are found in the network. Traditional cryptography schemes have gained popularity in secure communication and proved to be significant in identifying insider attacks. To address this issue, several researchers have proposed models and frameworks using a societal pattern called trust. Trust is the degree of belief about the behavior of other entities (or nodes). Each node in the network assesses the behavior of the neighboring nodes based on cooperation and coordination received in network operations such as packet forwarding, acknowledgments, maintaining packet integrity etc., [3][4][15].

Among routing protocols geographic routing offers guaranteed packet delivery in a dense network. Greedy Perimeter Stateless Protocol (GPSR) [5] is a geographic routing protocol which has proved its efficiency in self organized ad-hoc networks. Asad et al [6], have proposed an integrated trust model called Trusted GPSR (T-GPSR) in which a weighted trust model has been incorporated in GPSR protocol to bypass malicious nodes from routing. T-GPSR employs heuristic weight values to evaluate total trust value of neighboring nodes. However, heuristic assignment of weights provides flexibility but they are not suitable in the presence of several security attacks such as Grey hole, selfish behavior, on-off attack etc., are launched in the network in different proportions. To overcome this limitation, an improvement is suggested in this paper with an emphasis on trust update, lightweight trust computation and storage to reduce communication and storage overhead. Simulation study indicates that the packet delivery ratio of the improved T-GPSR (IT-GPSR) has improved by 10% over T-GPSR in the presence of

50% of malicious nodes in the network.

The rest of the paper is organized as follows: In Section II, trust concepts and previous work are presented. In Section III, the network model, security threats and the network performance metrics considered for evaluating IT-GPSR is presented. In Section IV, improved T-GPSR is presented. In Section V, the performance of IT-GPSR has evaluated with a simulation study. Finally, Section VI concludes the paper.

II. Trust Concepts and Previous Work

A. *Trust and its concepts*

Basically; trust is an abstract concept on which several definitions are provided in the literature. The concept of trust is used in various fields like psychology, sociology, anthropology, economics, political science, and computer science related fields such as e-commerce, social networks etc [2]. This concept has significantly gained attention in the field of communication to incorporate security. However, trust is utilized to define the degree of belief about the behavior of a particular entity. The trust calculation and establishment are carried out in association with routing protocols. While performing routing, every node maintains a trust table to keep track of the behavior of neighboring nodes to aid routing decisions. This helps in mitigating potential risks such as dead or ambiguous paths and security threats. The trust value can be useful to circulate a warning or alarm message among friend nodes. In case, if the trust value is very low then the node will be isolated from the network.

In a network, a node can obtain subjective observations about its neighbors [3]. In case, if a node calculates how much it trusts another node in a subjective manner then it is said to be direct trust. Whenever trust management is incorporated in routing, each node needs to observe neighboring nodes and predict the reputation by collecting evidences regarding behavior in discharging duties such as cooperation and integrity maintained in packet forwarding, acknowledgements, node energy consideration, distance measurement between neighbors etc. Trust of a node will improve whenever a node exhibits positive behavior or other nodes have positive experiences with it. However, these direct observations may become cumbersome whenever a malicious node responds to every query without performing the required operation. In this case, two nodes may gossip trust information about third node so that all the three nodes indirectly come to know each other trust information. This is said to be indirect trust. In addition to these two ways, nodes can obtain recommendations from the trusted third parties such as a base station or relay nodes or cluster heads. Hence, a node can obtain trust information either directly by first hand, indirectly by second hand in a distributed fashion or by receiving recommendations from trusted third parties in a centralized or hierarchical fashion.

During the initial stage of the network (i.e. after node placement and bootstrapping) each node exhibits positive behavior and cooperation. Security threats can be expected as the network operations progress. A foremost issue to be taken into consideration in this context is how to bootstrap trust. From the time of node bootstrapping, trust values can be gathered by nodes self experiences, direct observations (one hop neighbors), observations in coalition with neighbor nodes (multi hop) and by authenticating identity or certificates for every significant transaction [4].

B. *Greedy Perimeter Stateless Routing (GPSR)*

Greedy perimeter stateless routing (GPSR) [5] is a geographic routing protocol which performs routing by identifying neighboring node that is close to the destination. GPSR works with extensive use of locations information of nodes in the network. It works in two modes: Greedy mode and perimeter mode. In Greedy mode, an efficient path will be identified to reach destination. In perimeter mode, the routes are identified along the perimeter of the region. This mode is used when greedy mode fails to find a path towards destination. In addition, for routing decisions, GPSR maintains information related to distance of neighbors, link state of neighbors, and a path vector. All routing decisions are made with one hop information. The distance between neighbors is maintained through periodic beaconing location information. In mobile networks, a node may discover new nodes and its old neighbors can disappear. A fresh list of neighbors is maintained with periodic removal of dead nodes. A well known graph traversal rule called right hand traversal rule is employed in the protocol for perimeter forwarding of packets. During perimeter forwarding graph planarization techniques are used to avoid crossing lines in the network. A node identifies the state of the other node with promiscuous use of the network interface. Both greedy and perimeter methods provide full GPSR protocol. Perimeter mode operates on planar graph when the greedy mode on a full network graph fails.

C. *Trusted Greedy Perimeter Stateless Routing (T-GPSR)*

Trust concept has been incorporated in GPSR protocol (T- GPSR) in [6]. T-GPSR considers two service criteria: the number of packets forwarded P_f and number of packets forwarded without tamperingP_{wt}. The trust of a node j is calculated as

$$T(node_j) = W(P_f).P_f + W(P_{wt}).P_{wt} \tag{1}$$

Where, $W(P_f)$ and $W(P_{wt})$ are weights associated with two services. These weights are set heuristically based on the priority of particular service category. The service criteria P_f and P_{wt} are set to 1. Each positive observation is incremented by 1 (count of related service is incremented by 1) and negative observation is subtracted by 1 (count of related service is decremented by 1). Finally, for every trust update interval (TUI) the total trust $T(node_j)$ of neighboring node j is computed. During routing the data packets are forwarded to neighboring node with highest trust value.

Nael et al [7], has proposed a solution for security of geographical forwarding. It includes two parts; first, authors provided location verification to overcome location falsification attacks by placing relay nodes in the network. Second, technique to route authentication and trusted route discovery has been proposed. Ka et al [8], have proposed trust based on geographical scheme with a weight value associated with a packet and node agent. An agent forwards the packet only if it has trust value greater than trust associated with the packet.

III. Network Model, Security Threats and Network Performance Metrics

A. Network model

Let S be a set of n sensor nodes $S = (s_1, s_2, ..., s_n)$ deployed in a geographical region(x_i, y_i). These nodes interact directly with each other to forward the packets. In this model, it is assumed that each node has a unique identity and aware of its own location. Generally, location information will be obtained by installing Global Positioning System (GPS) or using any localization technique [9]. Each node in the network uses a symmetric key for encrypting the data and generating a Hash code for maintaining packet integrity. All the nodes will communicate using bidirectional transceivers. Each node takes advantage of promiscuous mode of the network interface. In promiscuous mode, a node can observe all packets passing through its radio range.

B. Security threats

In Ad hoc and sensor networks security attacks can occur in two ways [10-12] [18][19]. First, wireless networks are unreliable and more prone to eavesdropping. Jamming attack is one which comes under this category. In this attack, an intruder attempts to jam the signals by interfering with radio frequency used by nodes in the network. A way to mitigate these attacks is by varying the frequency spectrum of the signal. Second, since the nodes in WSN are left unattended, an intruder can attempt for physical capture of nodes, extract the secret information, reprogram the node and replace back to gain full control over the network. These re-programmed nodes exhibits deviated behavior of regular network operation and resulted as security attacks. Such security attacks can be classified as follows:

- *Selfish behavior:* An attacker relies on routing points, such as gateways or routing junctions, so that, packets forwarded by sensor nodes will be simply dropped, there by packets never reach destination. Generally, nodes exhibit selfish behavior to save energy.
- *Grey Hole:* In this attack a malicious node selectively forwards or drops the packets. In addition, a Grey Hole node can tamper the integrity of the packet so that the receiver node drop the packet as it is invalid.
- *On-off attack:* A malicious entity behaves well and worse alternatively so that they can remain undetected while causing damage in the network.
- *Modification Attack:* A malicious node modifies the packet integrity by tampering its unique code or Hash code so that a receiving node discards the packet as invalid.

In the IT-GPSR, it is assumed that threats are launched by malicious nodes after deployment of the network. In this work, all the above described security attacks are studied.

C. Performance metrics

The following network performance metrics are considered to evaluate the efficiency of the proposed model.

- *Packet Delivery Fraction:* It is the ratio of number of packets received by the destination node to the number of packets sent by the source node.
- *Packet Forwards:* It is the number of data packets that are successfully forwarded by the intermediate nodes.
- *Average hop count:* It is the mean number of hops that the data packets are traversed to reach their destination.

  Throughput: It is the mean data bits sent per second in the network.

IV. Improved T-GPSR (IT-GPSR)

In this section, IT-GPSR for secure geographic routing is described. Pseudo code for trust derivation and computation is provided in Fig 1. This model focuses on systematic weight assignment, systematic trust update, lightweight trust computation and storage to reduce communication and storage overhead. Without loss of generality, every node in the network maintains a neighbor table which keeps track of neighboring node identities and corresponding location information. In addition to it, every node maintains a packet buffer table which stores a copy of all outgoing data packets and forwarding node identity. Like T-GPSR, every node in the network keeps track of two service criteria; first, number of packets forwarded (P_f) and second, number of packets forwarded without modification (P_{wt}). Initially these two service criteria counters are initialized to 1

A. Systematic weight assignment

Every node switches its receiver into promiscuous mode each time they transmit a data or control packet (tap () function). With this switching, a node can overhear all ongoing packets in its transmission range. Let A and B are the sending and receiving nodes respectively, when node A transmits the data packet then it stores the copy of the packet in the packet buffer table and observes for the sent packet in promiscuous mode. If node A observes the transmitted data packet, then it verifies the packet integrity. If the packet integrity check fails then node A confirms that node B has performed modification attack. Otherwise, node A asserts that node B is a benign node. In addition to the observation related to modification attack, node checks for the benevolence showed in packet forwarding. With the positive observations, related service criteria counters are incremented and the negative observations related service criteria counters are decremented.

```
GPSR_ALIVE_EXPIRY = 3 * (bint_ + drate_ * bint_)
TUI = 2* GPSR_ALIVE_EXPIRY + random( bint_ * drate_)
init() {      // Initializing trust elements and scheduler
 int r_pf = 1;
 int s_pf = 1;
 int r_pwt = 1;
 int s_pwt = 1;
 int Pf = 1;
 int Pwt = 1;
 Trust_Scheduler(TUI);     // Scheduling trust update
}
// Data packet forwarding mechanism
forward(Packet *p) {
vector<PBuffer *> pbuf;   // Packet buffer table
  next_node = find_trusted_node();   // next node to forward
  // buffer the next node and packet in Packet buffer vector
  pubf->buffer(next_node, p->copy());
  schedule(p);        // Schedule the packet
}

// Routine to find trusted node to forward data packet
find_trusted_node() {
 next_node = -1;
 double tt_ = 0;
 for(i = 0; i < neighbor_count; i++) {
   // Skip if status is malicious
    if(node(i)->status == 1) continue;
   // compare the total trust and distance
    if(total_trust(i) > tt_ &&
                    distance(i) < distance(next_node)) {
            next_node = i;
            tt_ = total_trust(i);
     }
 }
// return the trusted next node
return next_node;
}

// Promiscuous tap mode
tap(const Packet *p) {
   last_hop = packet_header(p)->last_hop;
   for(i=0;i<pbuf.size();i++) {
     Pbuffer *pb = pbuf.get(i);
     if(pb->node_id == last_hop) {
        Pf ++;
        r_pf ++;
        if(isValidPacket(pb->packet)) {
            Pwt++;
            r_pwt ++;
         } else { Pwt--; s_pwt++; }
     }
   // remove entry from packet buffer
   pbuf.remove(i);
   }
}

// Routine for trust update interval
Trust_scheduler() {
 int bit_exp:4;
 double total_trust, exp_pf, exp_pwt;
 for (i=0;i<neighbor_table.size();i++) {
 // computing expectation of packet forwards
   exp_pf(i) = r_pf(i)/(r_pf(i) + s_pf(i));
 // computing expectation of packet integrity
   exp_pwt(i) = r_pwt(i)/(r_pwt(i) + s_pwt(i));
 // computing resultant expectation and reducing the size of
 // the resultant expectations.
   bit_exp(i) = ceil(((exp_pf(i)+exp_pwt(i))/2) * 10);
   // computing total trust
   total_trust(i) = exp_pf(i) * pf(i) + exp_pwt(i) * pwt(i);
   // declare node as malicious if total_trust < 1
   if(total_trust(i) < 1) status(i) = 1;
 }
init();
}
```

Fig 1. Integrated trust model derivation, computation pseudo code

With these values, the direct trust of node A on node B can be computed using Eq (1). The weights in the Eq (1) are set heuristically based on the priority of the service. For example, number of packets forwarded and packets forwarded without tampering are one (P_f=1 and P_{wt}=1) and corresponding weights are $W(P_f)$=0.25 and $W(P_{wt})$ =0.75 (according to [6]) then the total trust (TT) value is 1 (Eq.(1)). So, a node can be assumed trustworthy if it has trust value greater than one. In case of on-off and Grey hole attacks, a malicious node selectively drops or tampers the packets. If such attacks are launched in different proportions, for example, it is observed that P_f = 0 and P_{wt} = 1 then the total trust value is 0.75. In converse case, if P_f=1 and P_{wt}=0, then the total trust value of node becomes 0.25. In a network, the packet forwards and drop cannot be proportional in the presence of On-off, Sink hole, Black hole, Grey hole and modification attacks are launched in different proportions. Having a common weight throughout the network operation for a service criteria can not results into same importance over time. In mobility, a node may enter or leave the transmission range of observing nodes. So, there is a need for balancing the total trust with respect to weights in the presence of any kind of attacks in any proportion. In this connection, a modification is done in this paper that the weights should be adaptive rather than heuristic. It will be more realistic if the weights vary with time and service observations. Thus, the latest interaction has new weights and can lead to effective routing decisions. To meet this, in IT-GPSR, the weights are obtained through the Beta expectation [13-14]. During interaction and observations with neighbors, a positive experience (α) is rated as 1 and a negative experience (β) is rated as 0. Reputation score is the expectation value of Beta probability density function (PDF) . A Beta PDF denoted by $beta(p|\alpha,\beta)$ and can be expressed by using gamma function Γ.

$$beta(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha).\Gamma(\beta)}.p^{(\alpha-1)}.(1-p)^{(\beta-1)} \qquad (2)$$

Where, p is first order probability variable and $0 \le p \le 1, \alpha, \beta > 0$. The function is with the restriction that the probability variable $p = 0$ if $\alpha < 1$ and $p = 1$ if $\beta < 1$. Expectation is given by $E(p) = \alpha/(\alpha + \beta)$. Where α, β are ratings of r positive and s negative outcomes with $\alpha = r + 1$ and $\beta = s + 1$. The PDF $beta(p|\alpha,\beta)$ represents second order probability. The fist order variable p is continuous and$p \in [0,1]$. So, with the first order value$p$, PDF in Eq.(2) is very small hence meaning less. As a remedy to this situation one can make use of either $\int_{p_1}^{p_2} beta(p|\alpha,\beta)$ or simply by considering the expectation of$p$. A simple solution to compute the trust is by using expectation of p is given by.

$$E(p) = \frac{r+1}{r+s+2} \qquad (3)$$

The weights in Eq (1) is rewritten using Eq (3) as $W(P_f)$=$E(p_f)$ and$W(P_{wt}) = E(p_{wt})$, in the case if a node behavior is stable. Otherwise,$W(P_f) = 1 - (1/m_f)$ $W(P_{wt}) = 1 - (1/m_{wt})$ and $m_f \ge 1, m_{wt} \ge 1$. Where, m_f and m_{wt} are the number of interactions related to packet forwards and packet forwards without tampering.

These weights balance the observations to detect the malicious nodes and weight values are maintained between 0 and 1. Finally, the total trust of a neighboring node j is calculated as

$$TT(node_j) = E(P_f).P_f + E(P_{wt}).P_{wt} \quad (4)$$

B. Systematic trust updation

Trust update interval is a vital factor to be taken into account in trust models. After every TUI, a node reaches a conclusion on neighboring nodes based on their behavior. In [6], TUI value is set heuristically, however, there should be a systematic mechanism to decide TUI. Large gap between TUIs may not reach to good decisions. For example, among 50 nodes in a network, 10 nodes are sending data packets at a rate of 4 packets per second and TUI are set to 5 seconds, between two TUIs the total number of packets released from all sources will be 10*4*5=200. If several attacks are launched in different proportions in the network, then all sending nodes can get information about malicious nodes only after losing less than or equal to 200 packets. In mobile scenarios, when a node is moving in a terrain it can discover new neighbors and old neighbors may disappear. In such situations, if difference between two TUIs is large then observing nodes may disappear so that the trust computation of those nodes becomes meaningless. So in IT-GPSR, TUI value is set based on the data rate and beacon interval. When data rate is high the reduction in TUI value can help in improving the packet delivery ratio. In GPSR [5], if a node does not receive a beacon from its neighbors within a time period (also called beacon expiry or alive expiry period) of three times of beacon internal time then it considers that node as dead node and removes the entry from the neighbor table. Motivated from this method, in IT-GPSR, the TUI value is set based on data rate and beacon interval. It is formulated as TUI = 2 * GPSR_ALIVE_EXPIRY + U (drate_ * bint_), where, drate_ and bint_ are the data rate and beacon interval. U (.) generates a uniform random number between 0 and drate_*bint_. GPSR_ALIVE_EXPIRY is set as 3 * (bint_ + drate_ * bint_). This procedure pseudo code provided in Trust_scheduler() function in Figure 1. In case of static networks, TUI is set to 5.0 Seconds as set in [6].

C. Lightweight trust computation and storage

After having the expectation and count values of the services criteria, for every TUI, node computes total trust value of neighboring nodes. The trust computation and final TT value composed of floating point values which require more space to store in a node memory as compared to any other data type values. To overcome this, IT-GPSR employs lightweight trust computation and storage with expectation values. It is formulated as

$$TT = \lceil (\frac{E(P_w) + E(P_{wt})}{2}).10 \rceil \quad (5)$$

Where, $\lceil \cdot \rceil$ converts the computed value to next nearest integer. In other words, it performs ceil () operation. Since the expectation value is computed with positive and negative observations, count values of service criteria can be neglected. For example, with the Beta reputation system, if a node computes expectations as $E(P_f)$ = 0.75 and $E(P_{wt})$ = 0.5 then the TT value become 6 (Eq (5)). To store the obtained trust value 4-bit memory space is sufficient (4-bit can support from 0 to 15). Since the energy consumption in sensor nodes are computed based on the number of bits transmitted, the proposed technique can substantially reduce the energy consumption and at the same time communication overhead. In this way the total expectation is maintained between 0 and 1, and the TT value is maintained between 1 and 10.

Table 1: Simulation parameters

Examined Protocols	T-GPSR And It-GPSR
Simulation Time	600 Seconds
Simulation Area	1500 X 300 meters
Number Of Nodes	50
Transmission Range	250 meters
Mobility Model	Random way point
Maximum Speed	20 m/s
Traffic Type	CBR Over UDP
Maximum Connections	15
Packet Size	512 bytes
Packet Rate	4 packets/second
Maximum Malicious Nodes	25

Finally, several trust systems are designed with an option of broadcasting secondary trust information. However, it is disadvantageous in many cases. A malicious node can launch reputation based attacks such as ballot stuffing and bad mouthing [3]. Ballot stuffing is an attack in which a malicious node promotes itself with high trust value. Whereas in bad mouthing attack, a malicious node intentionally damages other nodes' reputation by continuously advertising poor trust value. In IT-GPSR, promoting second hand trust information is limited using piggybacking lower trust values (below 5) and related node identities on all data packets once for every TUI to reduce congestion in the network. Since all nodes operate in promiscuous mode, every node along the data packet forward path can overhear the secondary trust information. The observed secondary trust is updated with primary information to make efficient routing decisions.

V. Simulation Study

A. *Simulation environment*

The ns-2.35 [16] tool was used to evaluate the integrated trust model. Legacy code of GPSR [17] was ported to ns-2.35 and T-GPSR [6], IT-GPSR are built over it. Standard IEEE 802.11 Mac was used for simulation. The simulations were conducted on 25 static and dynamic random node topologies, and mean values of the results are presented. Beacon interval was set as a random value between 0.5 and 1.0 in dynamic networks. This paper assumes that security attacks are possible only after some time of network operation and the attacks are launched in incremental fashion. Security attacks described in section 2 are launched in incremental fashion in different proportions. Simulation parameters are listed in Table 1.

B. *Result Analysis*

Fig 2 (a) plots the packet delivery fraction (pdf) performance of IT-GPSR over T-GPSR and it is found that the pdf has steadily increased in IT-GPSR. In any malicious scenario, IT-GPSR exhibit minimum 8-10% improvement in pdf over T-GPSR. The results depict that IT-GPSR improved the packet delivery fraction up to 10% in the presence of 50% of malicious in the network.

Fig 2 (b) plots that the number of packets forwarded in the IT-GPSR is very high even in the presence of 50% of malicious nodes. IT-GPSR employs piggy backing second hand trust information. Each node in promiscuous mode monitors the information and updates their trust tables. Continuous availability of second hand information along with direct observations gives the ability to normal nodes to accurately identify the next best node. In addition, fresh trust information will be available on every node for every TUI period instead of a heuristic time period. This further enhances the ability of detecting the best next node to forward data. While forwarding packets, a node selects its immediate best neighbor based on trust values instead of nearer node to the destination. For every TUI, neighboring nodes with TT value less than 5 are labeled as malicious and discarded from searching next best node to forward data packets. So, a node looks for trustworthy node rather than the nearest node to the destination. It makes the packets to take additional routes than o packets. So, a node looks for trustworthy node rather than the nearest node to the destination. It makes the packets to take additional routes than optimal paths. Hence, it increases the average number of hops a packet can traverse. Taking additional paths can also lead to rising in packet forwards between source and destination. Fig 2(c) plots this result. The average hop count is stable and steadily decremented as the number of malicious nodes increases in the network. This means that IT-GPSR is able to find the next best node with high trust value in the shortest path between source and destination.

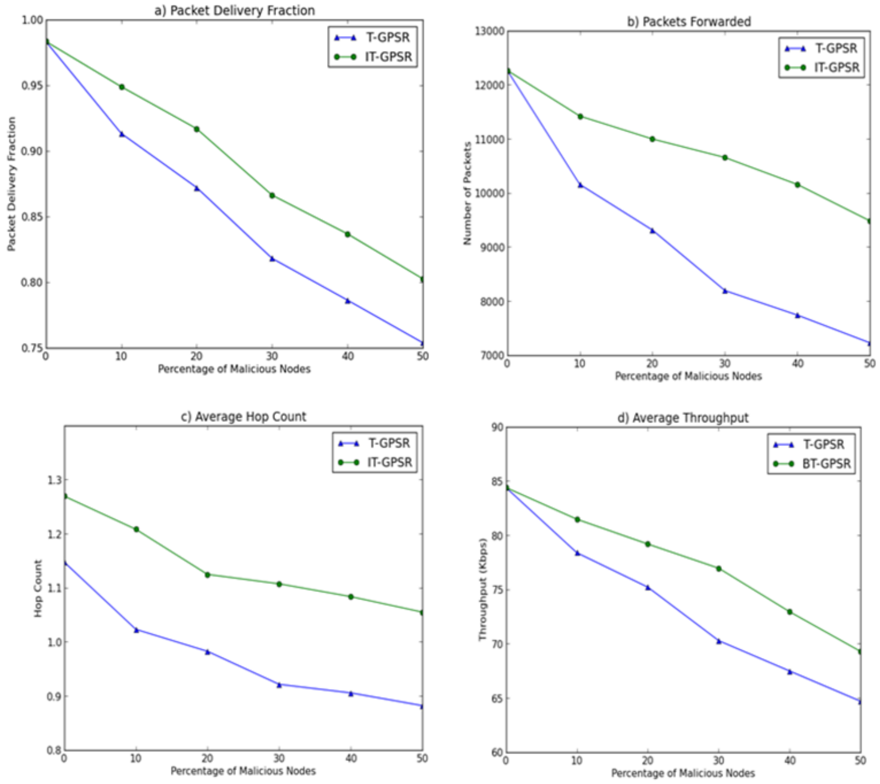

Fig.2. Network performance metrics. a) Packet delivery ratio b) Number of packet forwards c) Average hop count d) Average throughput

Fig 2 (d) plots that IT-GPSR result in increasing throughput. As the number of data forwards increase, number of data bits sent in the network also increases. IT-GPSR enables the nodes to increase the capability of suspecting a malicious node which drops or tampers the packets by updating the trust information for every TUI. It initiates a node to send data packets to the next trusted node to increase best-of-effort delivery.

VI. Conclusion

In this paper, an improved trusted greedy perimeter stateless routing (IT-GPSR) protocol has been proposed. This model is developed with an emphasis on trust update, lightweight trust computation and storage to reduce communication and storage overhead. Packet delivery fraction of the IT-GPSR has improved by 10 % in the presence of 50% of malicious nodes in the network. In addition, network performance metrics such as network throughput, average hop count, and data packets forwarded has improved over T-GPSR. The effect of Grey Hole and modification attacks is studied with IT-GPSR. However, in addition to these attacks, a serious threat to geographic routing called Sybil attack needs to be addressed. In Sybil attack, a malicious node intentionally broadcasts incorrect location information to disturb or attract the network traffic. Developing efficient models to deal with Sybil attack is left as future work.

References

[1] I.F.Akyildiz, W.Su, Y Sankarasubramaniam, E. Cayirci,"Wireless Sensor Networks: A Survey", Computer Networks, Elsevier, Pages 393-422, Volume 38, Issue 4, 15 March 2002.

[2] Kannan Govindan, Prasant Mohapatra," Trust computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys and Tutorials, vol 14, No 2, Second Quarter 2012.

[3] Marcela Mejia, Nestor Pena, Jose L Munoz, Oscar Espanza, "A Review of trust modeling in adhoc networks", Internet Research, Vol 19, issue 1, pp 88-104, 2010.

[4] M. Carmen Fern andez-Gago, Rodrigo Rom an, Javier Lopez, A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks", proceedings of Third International Workshop on SecPerU 2007.

[5] B. Karp and H. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in Proceedings of the 6th Annual ICMCN, ACM Press, 2000, pp. 243–254.

[6] AA Pirzada, C McDonald," Trusted Greedy Perimeter Stateless Rout-ing", proceedings of ICON 2007.

[7] Nael Abu Gazaleh, Kyoung Don Kang and Ke Liu, "Towards Resilient Geographic Routing in WSNs", Proceedings of Q2Winter, Oct 13, 2005.

[8] Ka-Shun Hung, King-Shan Lui, and Yu-Kwong Kwok, "A Trust Based Geographical Routing Scheme in Sensor Networks", proceedings of IEEE WCNC, March 2007.

[9] Wymeersch, H, Lien, J. and Win, M.Z., "Cooperative localization in wireless networks", Proceedings of the IEEE, Volume: 97, Issue: 2, Pages: 427 – 450, February 2009.

[10] Yanli Yu, Keqiu Li, Wanlei Zhou, Ping Li," Trust mechanism in wireless sensor networks: attack analysis and countermeasures", Journal of Network and computer Applications 35 (2012) 867-880.

[11] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Counter Measures", Ad hoc Networks, Special Issue on Sensor Networks protocols and applications, Elsevier Publication, Volume 1, Issues 2-3, Pages 211-350, September 2003.

[12] Aurlien Francillon, Claude Castelluccia," Code Injection Attacks on Harvard-Architecture Devices", proceedings of CCS08, October 2731, 2008.

[13] Audun Josang, Roslan Ismail, "The Beta Reputation System", proceedings of 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 17 - 19, 2002.

[14] Saurabh Ganeriwal and Mani B. Srivastava," Reputation-based model for High Integrity Sensor Networks", proceedings of SASN04, October 25, 2004.

[15] P. Raghu Vamsi and Krishna Kant, "Systematic Design of Trust Management Systems for Wireless Sensor Networks: A Review", proceedings of ACCT, 8-9 February, 2014.

[16] Network simulator ns-2 available at http://www.isi.edu/nsnam/ns.

[17] GPSR source code www.icir.org/bkarp/gpsr/gpsr.html.

[18] G.Jose Moses, P.Suresh Varma, N.Supriya, G.NagaSatish, "Security Aspects and Challenges in Mobile Adhoc Networks", IJCNIS, vol.4, no.6, pp.26-32, 2012.

[19] G.Sunayana, Sukrutharaj.M, Lalitha rani.N, M.B.Kamakshi, "Security Mechanisms to Decrease Vulnerability of Ad-hoc Routing Protocols", IJCNIS, vol.4, no.12, pp.65-72, 2012.

Authors' Profiles

P. Raghu Vamsi is a PhD candidate in Department of Computer Science and Engineering (CSE), Jaypee Institute of Information Technology (JIIT), Noida, India, from the year 2012. He received B.E in CSE from University of Madras, Chennai, India, M.Tech in Software Engineering from Kakatiya University, Warangal, India, and M.B.A in Human Resource Management from IGNOU, New Delhi, India, during the years 2003, 2007 and 2010 respectively. Before joining JIIT, he has 7 years and 6 months of experience in teaching in various engineering institutions. He is a student member of IEEE, ACM and life member of CRSI, ISTE India.

Krishna Kant, Ph.D., is Professor and Dean (Academic), Department of Computer Science and Engineering, Jaypee Institute of Information Technology, Noida, India. Earlier he served as Senior Director in the Department of Information Technology, Ministry of Communication and Information Technology, Government of India. He received his Masters in Physics (with specialization in Electronics) in the year 1972 from Jabalpur University, his Masters in Computer Science in the year 1975 from BITS Pilani, and his Ph.D. in Computer Science in the year 1980 from the Indian Institute of Technology Delhi. Dr. Krishna Kant has wide experience in designing and implementing microprocessor-based, real-time systems for different applications. He coordinated the UNDP project on Microprocessor Application Engineering Programme (MAEP) and was closely associated with the conceptualization and development of a number of agri-instrumentation systems at MAEP centre at JNKVV Jabalpur, India. He also imparted training to agriculture scientists on microprocessor applications. He taught "Microprocessor and Applications" and "Computer Control of Processes" courses to MCA and ME students, respectively, for three years in the University of Delhi, India. He has authored five books.