Abstract—Geographic routing offers guaranteed packet delivery in a dense network. In this routing, packets are forwarded to a node which is nearer to the destination with an extensive use of location information. However, research studies in Mobile Adhoc Networks (MANETs) and Wireless Sensor Networks (WSNs) have shown that packet delivery percentage can degrade substantially when malicious nodes are found in the network. Conventional cryptography techniques can be adopted in order to deal with malicious nodes, but they cannot mitigate outsider attacks. In recent years, a societal pattern called trust is used as a tool to mitigate security attacks. Numerous researchers have proposed security solutions by adopting trust in routing algorithms. However, each solution has its own strength and weakness. In this paper, an integrated approach by using reputation and weight based trust systems backed by Greedy Perimeter Stateless Routing (BT-GPSR) is presented. The proposed approach outperforms the conventional reputation and weight based methods. The effectiveness of the proposed BT-GPSR is validated through simulation.

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

I. INTRODUCTION

There are two special classes of wireless networks; Mobile Adhoc Networks (MANET) and Wireless Sensor Networks (WSNs). MANETs are self configurable networks in which nodes are connected by wireless links. Since MANETs are mobile, it results in frequent topological changes. Whereas WSNs are composed of low cost tiny sensor nodes with limited resource in-terms of processing, energy, memory and transmission range. However, WSNs are mostly static and operated in inaccessible environments. These networks consist of autonomous sensing and communication units called sensor nodes (SNs) (or simply nodes) whose task is to sense the environment and report the data to the base station (BS) in a single or multi hop fashion with localized routing decisions. To reduce the commercial cost, SNs are not covered with protected bodies. Applications of these networks include earthquake 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].

Limited transmission range of nodes restricts them to follow multi-hop communication to forward the data packets to the destination. The pattern of discovering a path from source to destination is said to be routing. Numerous researchers have designed routing protocols to suit a variety of applications. A defacto classification provided for these routing algorithms is 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. However, the communication can be guaranteed only with positive cooperation among nodes. But, limitations such as, wireless communication, lack of tamper proof bodies, unattended deployment etc., often lead to vulnerabilities and prone to security attacks. Traditional cryptography schemes have gained popularity in securing communication; they have proved to be significant in identifying insider attacks. In addition, these algorithms carry extensive computation and usually require thousands or millions of multiplication and addition operations to execute a single security operation. Hence, these are not suitable for resource constrained WSNs. So, there is a need to improve security while maintaining low resource consumption.

In this paper, an integrated trust system which can bypass and isolate malicious nodes is presented. This system is incorporated in to a well known geographic routing protocol called Greedy Perimeter Stateless Routing (GPSR)[11]. This model uses the features of reputation based trust system proposed in [5] and a weight based trust proposed in [6-8]. In addition, a lightweight trust system is used to keep track of trust information of neighboring nodes. Our design is based on trust assessment with reputation monitoring using direct and indirect observations. Moreover, our design integrates location awareness and a reputation system to achieve dependability, integrity and to scale large network dimensions.

The rest of the paper is organized as follows: In section 2, we present background and preliminaries to understand the paper. In Section 3, we explain the related work. In Section 4, we describe the network model, security threats and network performance metrics considered for evaluating our integrated model. In Section 5, our proposed integrating model (BT-GPSR) is presented. In Section 6, we analyze the performance of our proposed model with a simulation study. Finally, section 7 concludes the paper.
II. BACKGROUND AND PRELIMINARIES

A. Trust concepts

Research in the field of MANETs has shown that quality of service (QoS) is gradually affected when malicious nodes are found in the network. It turned the attention of researchers to adopt a societal pattern called trust. Similarities of MANETs with WSNs lead to inheriting trust models to work with WSNs. Basically, trust is an abstract concept on which several definitions are available 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 by predicting 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 completely low then the node will be isolated from the network.

A node can obtain subjective observations about its neighbors [9]. 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, energy depletion, distance measurement etc. Trust of a node will be improved whenever it 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 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, or by receiving recommendations from trusted third parties in a centralized or hierarchical fashion.

Trust has several properties. First, trust is not static; it is dynamic. Trust will be improved if any positive experiences take place and decreases in the opposite case. So, trust changes over time and type of transaction experienced. Second, trust is asymmetric which means two nodes may not have equal trust in each other. Third, trust is context dependent. The degree of trust will be built on context and application involved. The context or applications can be military surveillance, home automation, industrial applications etc. Fourth, trust is subjective. It has a quantifiable level or degree of belief over other nodes. Finally, trust is not transitive which means to let “→” is trust and A, B and C are three nodes, if A→ B, B→ C then A→ C is not guaranteed [10].

During the initial stage of the network (i.e. after node placement and bootstrapping) each node exhibits positive behavior and cooperation. Security threats, vulnerabilities and attacks can be expected as the network operations progress. A foremost issue to be taken into account 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 [11].

B. Greedy Perimeter Stateless Routing (GPSR)

Greedy perimeter stateless routing (GPSR) [12] is a geographic routing protocol which performs routing by identifying nearest neighbor 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. Whereas 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 three state informations such as distance of neighbors, link state of neighbors, and 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 disappear old nodes. 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 a network interface. Both greedy and perimeter methods provide full GPSR protocol. Perimeter mode operates on planarized graph when the greedy mode on a full network graph fails.

III. RELATED WORK

Historically, solutions to security issues in WSNs have been investigated by several researchers. However, it still remains a challenging problem. In order to bypass the compromised or malicious nodes, a multidisciplinary concept called trust management has been widely studied by scholars. Trust has become a significant aid in routing, data aggregation and intrusion detection. There exist numerous works to address security issues in MANETS and WSNs using trust [3-8]. In this section, we present related work for trust management in wireless ad hoc and sensor networks.

A. Arithmetic/Weighted mean trust model

Trust concept has been incorporated with GPSR (T- GPSR) in [13]. T-GPSR considers two service criteria: the number of packets forwarded \( P_f \) and number of packets forwarded without tampering \( P_{wt} \). The trust of a node is calculated as

\[
T(node_j) = (W(P_f) * P_f + W(P_{wt}) * P_{wt})
\]
where, \( W(P_f) \) and \( W(P_{we}) \) are weights associated with two services. Each node in the network observes the neighboring nodes for the two service criteria. Each positive observation is assigned value 1 (weight of related service is incremented by 1) and negative observation is assigned value -1 (weight of related service is decremented by 1). Data packets are forwarded to neighboring node with highest trust value.

In [7], weights are associated with a packet and agent. An agent can forward the packet only if it has trust value greater than trust associated with the packet. A generic method to calculate trust by multiplying direct and indirect trust is proposed in [14]. This method considers the product of trust as reputation. Product of past actions and observations are considered as direct reputation. Let A and B are two agents, A needs to observe B for certain service \( s \), at time \( t \) then the direct reputation of B is calculated as \( DR_t A(B|s) = F_1(t,T_i) \ast g_k \). Where, \( F_1(t,T_i) \) is a time dependent function and \( g_k \) is the number of successful observations. \( F_1 \) gives higher relevance to the observed values of \( g_k \). Indirect reputation will be calculated in a similar way by collecting information from friend nodes. Finally, total reputation is calculated as

\[
TR = W_k \ast (DR_t A(B|S_k) + IR_t A(B|S_k))
\]

Where, \( W_k \) is weight associated with service \( S_k \). These weights are set heuristically between 0 and 1.

B. Reputation based trust model

A node in the network can forward data packets successfully when there exists positive cooperation from its neighbors. Each node will observe its neighbors to understand network environment. With these observations, trust values of neighboring nodes are computed. During interaction and observations with neighbors, a positive experience \( (\alpha) \) is rated as 1 and a negative experience \( (\beta) \) is rated as 0. Reputation score is the expectation value of beta probability density function (betaPDF) [16]. A beta PDF denoted by \( \text{beta}(p|\alpha,\beta) \) and can be expressed by using gamma function \( \Gamma \). It is expressed as

\[
\text{beta}(p|\alpha,\beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{(\alpha - 1)}(1 - p)^{(\beta - 1)}
\]

Where, \( p \) is probability variable and \( 0 \leq p \leq 1, \alpha, \beta > 0 \). 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 \( \alpha, \beta \) are ratings of \( r \) positive and \( s \) negative outcomes with \( \alpha = r+1 \) and \( \beta = s+1 \). A quantitative trust establishment model proposed in [15] takes advantage of this method. The behavior of nodes is unpredictable or uncertain in the network dynamics. To predict the behavior, Bayesian theory is used to make use of prior probability of events and is later updated in the light of collected or available evidence. So, it is best suitable where uncertainty is present in node behavior. In [5], a beta reputation system is developed by using the Beta probability density function (PDF). It models posterior reputation value by taking binary ratings as input.

IV. NETWORK MODEL, SECURITY THREATS AND PERFORMANCE METRICS

A. Network model

Let \( S \) be a set of \( n \) sensor nodes \( S = \{s_1, s_2, \ldots, s_n\} \) deployed in a geographical region \( (x_1, y_1, \ldots, x_n) \). 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). 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 with bidirectional transceivers. Each node makes use 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 [2]. First, wireless networks are unreliable and more prone to eavesdropping. Jamming attack is one which comes under this category. In this, 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 from regular network operation. Such deviated behaviors can be classified as follows:

1) Sink Hole: A malicious node creates an impression as the next node to forward packets. There by malicious node drops the packets by attracting traffic from neighboring nodes.
2) 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 the destination. Nodes exhibit selfish behavior to save energy.
3) Grey Hole: It is a variant of Sink hole attack in which 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.
4) On-off attack: A malicious entity behaves well and worse alternatively so that they can remain undetected while causing damage in the network.
5) Modification Attacks: 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 our integrated model, it is assumed that threats are launched by malicious nodes after deployment of the network. In this work, threats such as sink hole, Grey hole, selfish behavior, on-off behavior and modification attacks are considered for study.
Let $r, s$ are number of positive and negative observations, the Beta expectation is calculated as [5].

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

(4)

So, we set $W(P_f) = E(p)$ and $W(P_{wt}) = (1 - E(p))$ in case if a node behavior is stable. Otherwise, we set $W(P_f) = 1-(1/m)$, $m \geq 1$, and $W(P_{wt}) = (1 - E(p))$ where $m$ is the number of observations. This weight balance the observations to detect the malicious nodes.

Basically, trust value of other nodes is computed for a fixed time interval (also said to be trust update interval (TUI)). In [13], TUI value is set heuristically. However, there is no mechanism to decide the TUI. In our model, TUI value is set based on the data rate. For example, 10 nodes are sending data packets at a rate of 4 packets per second and TUI is set to 5 seconds, between two TUIs the total number of packets released from all sources will be $10^4*4*5=200$. Which mean a node can get the information about a malicious node only after losing less than or equal to 200 packets. When data rate is high the reduction in TUI value can help in improving the packet delivery ratio. In GPSR, if a node does not receive a beacon from its neighbors with in a time period (also called beacon expiry period) then it considers that node as dead node and removes the entry from the neighbor table. There is a systematic method developed in [11] to decide the beacon expiry period based on beacon interval. In this model, the TUI value is set based on data rate and beacon interval. It is formulated as follows:

$$TUI = 3 \ast (bint + drate \ast bint).$$  

(5)

Where, $drate$ is data rate (fraction of packets per second), $bint$ is beacon interval. In case of static networks, TUI is set to 4.5 seconds as set in [12].

A node can request trust information about another node for second hand information. Researchers have used separate beacons to spread secondary information. However, such beacons create additional overhead and increase congestion in the network. In addition, second hand information contains trust information in terms of floating point values. For example, in beta reputation system, if a node experiences 8 positive observations and 2 negative observations then the reputation expectation is $E(p) = 0.75$ ($r = 8$ and $s = 2$ (using Eq(4))). The obtained expectation represents floating point value which requires more storage space. In our model, a technique to reduce the size of storage is proposed. The expectation value is set to $E(p) = \text{ceil}(E(p) \ast 10)$. This expectation value will return in terms of integer. Let us consider the obtained expectation 0.75, it can be set to $E(p) = \text{ceil}(0.75 \ast 10)$ which gives the value 8. To store the obtained trust value 4-bit memory space is sufficient (4-bit can support from 0 to 15 values). Since the energy consumption in sensor nodes are computed based on the number of bits transmitted, proposed technique can substantially reduce the energy consumption and at the same time communication overhead.

In the literature, 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. Ballot stuffing is an attack in which a malicious node promotes itself with high reputation value. Where, in bad mouthing, a malicious node intentionally damage other nodes reputation by continuously advertising poor trust value. In our design, we limit promoting second hand trust information using unicast messages. In addition, our design employs piggy backing trust information on all data packets 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.

VI. SIMULATION STUDY

A. Simulation Environment

The ns-2.35 [17] tool was used to evaluate the integrated trust model. Legacy code of GPSR [18] was ported to ns-2.35 and beta reputation and T-GPSR[13] are built over it. For discussion, Beta reputation model of GPSR is named as (B-GPSR), trusted GPSR is named as (T-GPSR) and our integrated trust model is named as BT-GPSR here after. Standard IEEE 802.11 Mac was used for simulation. The simulations were conducted on 15 static and dynamic random node topologies, and mean values of the results are presented. We set beacon interval as a random value between 0.5 and 1.0 for dynamic networks. The simulation parameters are listed in Table 1.

B. Result Analysis

The performance of BT-GPSR protocol is compared with the B-GPSR and T-GPSR are shown in the figure 1. The results depict that BT-GPSR improves the packet delivery fraction upto 10% in the presence of 50% of malicious nodes in the network.

The number of packets forwarded in the BT-GPSR is very high even in the presence of 50% of malicious nodes. BT-GPSR employ 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 to every node for every TUI period instead of a heuristic time period. This further enhances the ability of detecting the best succeeding 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. 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 rise in mean latency of reaching the packet to the destination.

BT-GPSR protocol 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. This results in increasing throughput in BT-GPSR protocol.

VII. CONCLUSION

In this paper, an integrated trust model for securing wireless ad hoc and sensor networks was designed and implemented. This model is designed by integrating the beta reputation system and weighted trust model. Simulation results have demonstrated that our model outperforms the beta and weighted trust models. The network performance metrics such as packet delivery fraction, network throughput, average hop count, and data packets forwarded has improved over the conventional methods. The effect of sink hole, Grey Hole, on-off and modification attacks is studied with BT-GPSR. However, in addition to these attacks, a serious threat to geographic routing called Sybil attack needs to address. 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 a part of our future work.

REFERENCES