IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Special Issue-3, May 2016 E-ISSN: 2347-2693

An Incentive And Trustworthy Systems With E-Star For Heterogenous Multihop Wireless Networks

Megha Rani R[1], Harshavardhan H [2]

[1,2] *Computer Science and Engineering, Srinivas Institute of Technology, Mangalore, India*

Available online at: www.ijcseonline.org

Abstract— For establishing stable and reliable routes in heterogeneous multi-hop wireless networks (HMWNs) a secure protocol for Establishing STable and reliable Routes (E-STAR) is proposed. It integrates incentive and trust systems with a trust-and energy-aware routing protocol. Compensating the nodes that relay others packets and charge those that send packets are main aims of incentive systems. The nodes competence and reliability in relaying packets in terms of multi-dimensional trust values are main attractions. The trust values are attached to the nodes public-key certificates to be used in making routing decisions. Two routing protocols is developed to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can prompt the nodes in maintaining route stability and reporting correct battery energy capability. Because any loss of trust will result in loss of future gains. Moreover, for the efficient implementation processing the incentive receipts for computing trust values are necessary. Analytical results demonstrate protocol is without false allegations. Improvement in the packet delivery ratio and route stability are proved through simulation results.

Keywords— Securing heterogeneous multi-hop wireless networks, packet dropping and selfishness attacks, trust systems, and secure routing protocols

I. INTRODUCTION

In multi-hop wireless networks, mobile nodes relies on the other nodes to relay the packets [1] in order to communicate. By using limited power and by improving area spectral efficiency packet transmission in Multihop can extend the network coverage area. At low cost the network can be deployed more readily. Heterogeneous Multihop Wireless Networks (HMWNs) involve in the implementation of useful applications such as data sharing and multimedia data transmission [2]. For example, users in one area having different wireless enabled devices can establish a network to communicate, distribute files, and share information. And also useful in military and disaster-recovery applications where the nodes' behavior is highly predictable because the network is closed and the nodes are controlled by one authority.

It is considered heterogeneous multi-hop wireless networks (HMWNs), where the nodes' mobility level and hardware/energy resources may vary greatly. However, the nodes' behavior is unpredictable in civilian applications for different reasons. The nodes are typically autonomous and self-interested and may belong to different authorities. The nodes also have different hardware and energy capabilities and may pursue different goals. In addition, malfunctioned nodes frequently drop packets and break routes due to faulty hardware or software, and malicious nodes actively break routes to disrupt data transmission. Since the mobile nodes are battery driven and one of the major sources of energy consumption is radio transmission, selfish nodes are unwilling to lose their battery energy in relaying other users' packets. For example, PDAs may not be able to relay packets effectively due to the scarcity of resources. In HMWNs, a route is broken when an intermediate node moves out of the radio range of its neighbors in the route. In addition, some nodes may break routes because they do not have sufficient energy to relay the source nodes' packets and keep the routes connected. Only one intermediate node can break a route, and a small number of incompetent or malicious nodes can repeatedly break routes. When a route is broken, the nodes have to rely on cycles of time-out and route discoveries to re-establish the route. These route discoveries may incur network-wide flooding of routing requests that consume a substantial amount of the network's resources. Breaking the routes increases the packet delivery latency and may cause network partitioning and the multi-hop communication to fail.

In the existing system Trust systems have been used in a wide range of applications, including public key authentication, electronic commerce, supporting decision making, etc. In HMWNs, trust management is essential to assess the nodes' trust worthiness, competence, and reliability in relaying packets. A node's trust value is defined as the degree of belief about the node's behavior, i.e., the probability that the node will behave as expected. The trust values are calculated from the nodes' past behaviors and

Corresponding Author: *Mr. Harshavardhan H*
Department of CSE, Srinivas Institute of Technology, Mangalore, India.

used to predict their future behavior. For example, there is a strong belief that a node will break a route if it broke a large percentage of routes in the past. Most of the existing trust systems in multi-hop wireless networks compute a single trust value for each node. However, a single measure may not be expressive enough to adequately depict a node's trustworthiness and competence. The payment system is not sufficient to ensure route stability. It can stimulate the rational nodes to not break routes to earn credits, but the routes can be broken due to other reasons. Examples for these reasons include low resources, node failure, and malicious attacks.

The proposed system proposes E-STAR, a secure protocol for Establishing STAble and reliable Routes in HMWNs. E-STAR integrates trust and payment systems with a trust-based and energy aware routing protocol. The payment system uses credits to charge the nodes that send packets and reward those relaying packets. Since a trusted party may not be involved in the communication sessions, an online trusted party (TP) is required to manage the nodes' credit accounts. The nodes compose of proofs of relaying packets, called receipts, and submit them to TP. Trust management is essential to assess the nodes' trustworthiness, competence, and reliability in relaying packets. A node's trust value is defined as the degree of belief about the node's behavior, i.e., the probability that the node will behave as expected. To propose a trust system that maintains multi-dimensional trust values for each node to evaluate the node's behavior from different perspectives. Multi-dimensional trust values can better predict the node's future behavior, and thus help make smarter routing decisions.

Two routing protocols trust-based and energy-aware are developed, called the Shortest Reliable Route (SRR) and the Best Available Route (BAR).The SRR protocol establishes the shortest route that can satisfy the source node's requirements including energy, trust, and route length. Whereas BAR protocol, the destination node may learn multiple routes and establishes the most reliable one.

Advantageous of this proposed system is that E-STAR integrates payment and trust systems with the routing protocol with the goal of enhancing route reliability and stability. To propose a multi-dimensional trust system based on processing the payment receipts. E-STAR stimulates the nodes not only to relay others' packets even if they have many credits, but also to stabilize the routes and report their energy capability truthfully to increase their chance to participate in future routes. Trust-based and energy-aware routing protocols are used to establish stable routes. Unlike most of the existing schemes that aim to identify and mitigate the malicious nodes, ESTAR aims to identify the good nodes and select them in routing. Improve the packet delivery ratio due to establishing stable routes.

The rest of the paper is organized as follows: Section II presents several related works found as a literature review, while Section III shows the system model. Section IV gives the proposed model. Finally, Section V concludes the paper.

II. RELATED WORK

A. Reputation-Based Schemes

Reputation-based schemes [3] attempt to identify the malicious nodes that drop packets with a rate more than a pre-defined threshold in order to avoid them in routing. These schemes suffer from false accusations where some honest nodes are falsely identified as malicious. This is because the nodes that drop packets temporarily, e.g., due to congestion, may be falsely identified as malicious by its neighbors. In order to reduce the false accusations, the schemes should use tolerant thresholds to guarantee that a node's packet dropping rate can only reach the threshold if the node is malicious. However, this increases the missed detections where some malicious nodes are not identified. Moreover, tolerant threshold enables the nodes with high packet dropping rate to participate in routes, and enables the malicious nodes to circumvent the scheme by dropping packets at a rate lower than the scheme's threshold. Using a threshold to determine the trustworthiness of a node is not effective in HMWNs because the nodes' packet-dropping rates vary greatly. Therefore, these schemes cannot guarantee route stability or reliability in HMWNs.

B. Incentive Schemes

Incentive or (payment) schemes use credits (or micropayment) to encourage the nodes to relay others' packets [4] [5]. Since relaying packets consumes energy and other resources, packet relaying is treated as a service which can be charged. The nodes earn credits for relaying others' packets and spend them to get their packets delivered. In Sprite, for each message, the source node signs the identities of the nodes in the route and the message. Each intermediate node verifies the signature and submits a signed receipt to TP to claim the payment. However, the receipts overwhelm the network because one receipt is composed for each message. To reduce the receipts' number, PIS [6] generates a fixed size receipt per route regardless of the number of messages. In ESIP [7], the payment scheme uses a communication protocol that can transfer messages from the source node to the destination with limited use of the public key cryptography operations. Public key cryptography is used for only one packet and the efficient hashing operations are used in next packets. Payment [8] is used to thwart the rational packet-dropping attacks, where the attackers drop packets because they do not benefit from relaying packets. A reputation system is also used to identify the irrational packet-dropping attackers once their packet- dropping rates exceed a threshold.

C. Trustworthy Systems

Theodorakopoulos et al [9] analyses the issue of evaluating the trust level as a generalization of the shortest-path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. The main goal is to enable the nodes to indirectly build trust relationships using exclusively monitored information. Velloso et al [10] have proposed a human-based model which builds a trust relationship between nodes in ad hoc network. Without the need for global trust knowledge, they have presented a protocol that scales efficiently for large networks. Lindsay et al [11] have developed an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. Trust is a measure of uncertainty with its value represented by entropy. The evidence collected for malicious and benign behaviors are probabilistically mapped by following a modified Bayesian approach. The probabilistic estimate of Bayesian approach is then mapped to entropy. A secure routing protocol with quality of service support has been proposed. The routing metrics are obtained by combing the requirements on the trustworthiness of the nodes and the quality of service of the links along a route.

III. SYSTEM ARCHITECTURE

A. Network Model

The considered HMWN has mobile nodes and offline trusted party whose public key is known to all the nodes. The mobile nodes have different hardware and energy capabilities. The network is used for civilian applications, its lifetime is long, and the nodes have long relation with the network. Thus, with every interaction, there is always an expectation of future reaction. Each node has a unique identity and public/private key pair with a limited-time certificate issued by TP. Without a valid certificate, the node cannot communicate nor act as an intermediate node. TP maintains the nodes' credit accounts and trust values. Each node contacts TP to submit the payment receipts and TP updates the involved nodes' payment accounts and trust values.

B. Antagonist Model

The antagonist have full control on their nodes which can change the nodes' normal operation and obtain the cryptographic credentials. They attack the incentive system to steal credits, payless, or communicate for free. Some competitors may report incorrectly related to their energy capability to increase their chance to be selected in routing protocol, e.g., to earn more credits. They also attack the trust system to falsely augment their trust values to increase their chance to participate in routes. They may try to defame other nodes' trust values. Rivals may launch denial-of-service attacks by breaking the communication routes intentionally. The mobile nodes are probable attackers but TP is fully secure. The nodes are autonomous and self-interested and thus motivated to misbehave, but TP is run by an operator that is interested in ensuring the network secure operation.

IV. PROPOSED MODEL

Fig. 1 shows that E-STAR has three main phases. The proposed E-STAR protocol consists of Data transmission phase, update credit and trust value phase and route establishment phase.

In Data Transmission phase, the source node chooses the destination node to which messages are to be sent. In order to establish the stable and reliable route the Update Credit-Account and Trust Values phases is used where TP determines the charges and rewards of the nodes and updates the nodes' trust values. Finally, in Route Establishment phase, trust-based and energy-aware routing protocol establishes stable communication routes.

A. Data Transmission Phase

The source node NS sends messages to the destination node ND through a route with the intermediate nodes NX; NY, and NZ as in fig.2 using the routing protocols discussed in section 3.5. Firstly the source node computes the signature ξs (i) = $\{H (H (m_i), ts, R, i)\} K_{s+}$ and sends the packet $<R, ts, i, m_i,$ ξs (i)> to the first node in the route. It contains the time stamp and the *i*th message. H (d) is the hash value resulted from hashing the data d using the hash function H (). {d} K_{s+} is the signature of d with the private key of NS. The purpose of the source node's signature is to ensure the message's authenticity and integrity and secure the payment by enabling TP to ensure that source node has sent messages. Each intermediate node verifies ξs (i) and stores ξs (i) and $H (m_i)$ for composing the receipt. Signing $H (m_i)$ instead of m_i can reduce the receipt size because the smaller-size $H (m_i)$ is attached to the receipt instead of m_i. The destination node further generates a one-way hash chain by iteratively hashing a random value h_S to obtain the hash chain $\{h_S; h_{S-1}; . . . ; h_1; h_0\}$ where $h_{S-1} =H (h_i)$ for $1\leq i \leq S$ and h_0 is called the root of the hash chain. The node signs h_0 and R to authenticate the hash chain and link it to the route, and sends the signature to the source node in route establishment phase. In order to acknowledge receiving the message, the destination node sends ACK packet containing the preimage of the last released hash chain element.

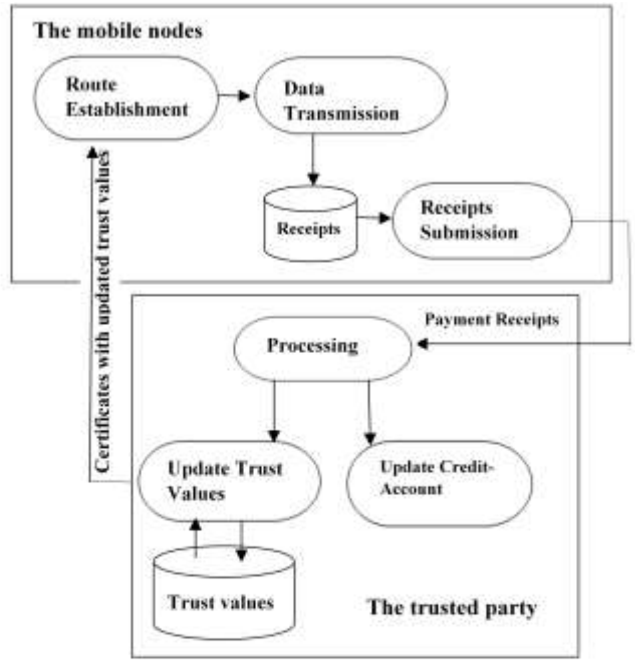

Figure 1 : The architecture of E-STAR

Each node in the route composes a receipt and submits it when it has a connection to TP to claim the payment and update its trust values. A receipt is a proof for participating in a route and sending, relaying, or receiving a number of messages. A receipt contains *R, ts, i, H* (m_i), $h_{0,}$ h_i, C_m, and an undeniable cryptographic token for preventing payment manipulation. C_m is data that depends on the used routing protocol, such as the number of messages the intermediate nodes commit to relay. The cryptographic token contains the hash value of the last source node's signature and *Auth_Code. Auth_Code* is the authentication code that authenticates the hash chain and the intermediate nodes to hold them accountable for breaking the route.

B. Update Credit Account and Trust Values Phase

Once TP receives a receipt, it first checks if the receipt has been processed before using its unique identifier *(R, ts).* Then, it verifies the credibility of the receipt by computing the nodes' signatures (ξs (i) and *Auth_Code*) and hashing them. The receipt is valid if the resultant hash value is identical to the receipt's cryptographic token. TP verifies the destination node's hash chain by making sure that hashing h_i *i* times produces h_0. TP clears the receipt by rewarding the intermediate nodes and debiting the source and destination nodes. The number of sent messages (*i*) is signed by the source node and the number of delivered messages can be computed from the number of hashing operations to obtain h_0 from h_i.

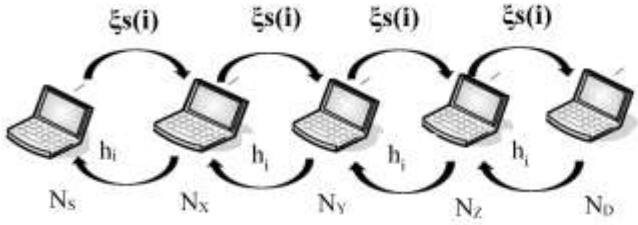

Figure 2 : The exchanged cryptographic tokens during data transmission

The notion of trust used in this paper is defined as the degree of belief, the expectation, or the probability that a node will act in a certain way in the future based on the nodes past behavior [6]. Trust values are calculated from the past behavior to predict the expected future behavior. For instance, people will not assign critical jobs to someone with a record of failure since there is a good reason to believe that he will not get the job done properly. Similarly, if a node has broken a large percentage of routes in the past, there is a strong belief that this node will break routes with high probability in the future, and thus the routing protocol should avoid it. The trust values are computed to depict the nodes' reliability and competence in relaying packets. A node can protect its trust values by not involving itself in routes with a neighbor that frequently breaks routes or has low trust values. Additionally, we are sure that the nodes that are not in a broken link did not break the route, which coincides with our objective of identifying good nodes.

Our trust system adopts multi-dimensional trust management framework in which the notion of trustworthiness is further classified into several attributes (or dimensions). Each attribute can indicate to what extent the node will conduct one specific action. We use multi-dimensional trust values instead of one trust value to precisely predict the nodes' future behavior. The trustworthiness of a node N_k is assessed in n-dimensional vector of numeric values $\tau_k = [\tau_k^{(1)}, \tau_k^{(2)},\ldots..\tau_k^{(n)}]$, where $\tau_k^{(i)}$, k stands for the *i*-th dimension of the trustworthiness of N_k. Each dimension $\tau_k^{(i)}$ corresponds to one action $\beta_k^{(i)}$. $\tau_k^{(i)}$ depicts the probability that N_k will conduct $\beta k^{(i)}$ in an appropriate manner, and thus the higher the value of $\tau_k^{(i)}$ is, the more likely N_k will conduct $\beta_k^{(i)}$. $\tau_k^{(i)}$ can be assigned any real value in the range of [0, 1] signifying a continuous range from complete distrust (0) to complete trust (+1), i.e., $\tau_k^{(i)} \in [0, 1]; \forall i \in \{1, 2\ldots.n\}$.

C.. Route Establishment Phase

In this phase, we present two routing protocols called the shortest reliable route and the best available route. SRR establishes the shortest route that can satisfy the source node's trust, energy, and route-length requirements, but the destination node selects the best route in the BAR protocol. The routing protocols have three processes: 1) route request packet (RREQ) delivery; 2) Route selection; and 3) route reply packet (RREP) delivery.

1) *The SRR Routing Protocol*

To establish a route to the destination node ND, the source node NS broadcasts RREQ packet and waits for RREP packet. The source node embeds its requirements in the RREQ packet, and the nodes that can satisfy these requirements broadcast the packet. The destination node establishes the shortest route that can satisfy the source node's requirements. The rationale of the SRR protocol is that the node that satisfies the source node's requirements is trusted enough to act as a relay. [13] The protocol is useful to establish a route that avoids the low-trusted nodes.

2) *The BAR Routing Protocol*

The nodes are motivated to report correct energy commitments to avoid breaking the route and thus degrading their trust values. Blind RREQ flooding generates few routes because each node broadcasts the packet once, which disables potential better routes. To solve this issue, BAR allows each node to broadcast the RREQ more than once if the route reliability or lifetime of the recently received packet is greater than the last broadcasted packet. The route lifetime is the minimum number of packets the intermediate nodes commit to relay.

To reduce the number of RREQ broadcastings, when an intermediate node receives a RREQ, it introduces a Wait Period to collect subsequent packets, if any, traveling through different routes and then selects some. It selects the most reliable route having at least lifetime of E_r *(S)*; and if this route does not exist, it selects multiple RREQ packets with at least total lifetime of E_r *(S)* in such a way that reduces the RREQ packets' number and maximizes the reliability.

After receiving the first RREQ packet, the destination node waits for a while to receive more RREQ packets if there are. Then, it selects the best available route if a set of feasible routes are found [12]. If there are multiple routes with lifetimes at least E_r *(S)* the destination node selects the most reliable route, otherwise, it establishes multiple routes with at least total lifetime of E_r *(S)* in such a way that reduces the routes' number and maximizes the reliability. The destination node should not select multiple routes with common node(s) (if possible) to disallow one node to break the routes.

V. CONCLUSION

We have proposed an Incentive and Trustworthy systems with E-STAR that uses payment/trust system with trust-based and energy-aware routing protocol to establish stable/reliable routes in HMWNs. E-STAR combines the nodes not only to relay others' packets but also to maintain the route stability. It also dismisses the nodes that report incorrect energy capability by reducing their chance to be elected by the routing protocol. We have also proposed SRR and BAR routing protocols and evaluated them in terms of overhead and route stability. Our protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behavior, and the route lifetime based on the nodes' energy capability. SRR establishes routes that can meet source nodes' trust/energy requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. For BAR, destination nodes establish the most reliable routes but with more overhead comparing to SRR. Analytical results demonstrate protocol is without false allegations. Improvement in the packet delivery ratio and route stability cane be achieved using the simulation results.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani and Kamal Bunkar, "An Overview & Study of Security Issues in Mobile Ado Networks", International Journal of Computer Science and Information Security (IJCSIS) USA, Vol-9, No.4, pp (106-111), April 2011

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.

[4] X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, "Autoregressive Trust Management in Wireless Ad Hoc Networks," Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3, pp. 229-242, 2012. SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no. 2, pp. 4–18, Apr. 2005.

[5] Neeraj Kumar Pandey and Amit Kumar Mishra, "An Augmentation in a Readymade Simulators Used for MANET Routing Protocols: Comparison and Analysis", International Journal of Computer Sciences and Engineering, Volume-02, Issue-03, Page No (60-63), Mar -2014

[6] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System For Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[7] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.

[8] M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.

[9] G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[10] P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, “Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model,” IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172-185, Sept. 2010.

[11] Harkiranpreet Kaur and Rasneet Kaur, "To Study the Various Attacks and Protocols in MANET", International Journal of Computer Sciences and Engineering, Volume-04, Issue-04, Page No (210-212), Apr -2016, E-ISSN: 2347-2693

[12] Mohamed M.E.A. Mahmoud, Xiaodong Lin, and Xuemin (Sherman) Shen, “Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks,” IEEE transactions on parallel and distributed systems, vol. 26, no. 4, April 2015

[13] A.Sreelatha , Dr.A.VinayaBabu , K.Madhukar , S.Nagaprasad , D.Marlene Grace Verghese , V.Mallaiah , A.Pratima ,” Mobile Wireless Enhanced Routing Protocol in Adhoc Networks” IJCSE, 2010; 2(7) 2398–2401

AUTHORS PROFILE

Megha Rani R received the B.E Degree in Information Science and Engineering from Mangalore Institute of Technology and Engineering, Moodbidri of VTU University Belagavi. She is currently pursuing her Master of Technology Degree in Computer Network Engineering at Srinivas Institute of technology Mangalore of Visveswaraya Technological University Belagavi. Her interests are in Computer networking, Communication technology aspects.

Harshavardhan H received the B.E Degree in Computer Science and Engineering from Jawaharlal Nehru National College of Engineering, Shimoga of Visveswaraya Technological University Belagavi. He has also received his Master of Technology Degree in Computer Science and Engineering from Manipal Institute of Technology Manipal University, Manipal. He is working as an Associate Professor from Past Ten years in Srinivas Institute of Technology, Mangalore. His areas of interest are in Computer networks, Software Engineering, and Image processing. He has published a paper in International Conference on Emerging Trends in Engineering Sciences 2015 and received best paper award for the paper entitled "Creation of Mosaic Image and Data Hiding for Transmission" held at Jain College of Engineering. He has presented a paper in International Conference entitled "CP-ABE in Decentralized Disruption- Tolerant Military Networks for Secure Retrieval of Data held at RV College of Engineering. He has also Presented a paper entitled "Dynamics of Modeling in Data Mining: Interpretive Approach to Bankruptcy Prediction" in National Conference on Knowledge based Computing Systems & Frontier Technologies-NCKBFT, held at Manipal Institute of Technology, Manipal.