# Learning the Channel Uncertainty for Defensive Security Enhancements in MANET with Trust Management

[1]Varad A. Sarve, [2]Dr. Swati S. Sherekar, [3]Dr. Vilas M. Thakare
[1,2,3]*PG Dept. of Comp. Sci. & Engg. ,SGBAU, Amravati,Maharashtra, India*

***Abstract***

*MANET incorporates many features such as dynamic topology and open wireless medium which are potential to security vulnerabilities. To avoid unintentional interferences, approaches must be examined as a promising complement to current cryptographic techniques. A trust management system, an interference model and some defensive methods can complete the requirement of modern networks altogether for better security. In this paper, an approach which can merge these elements is presented. A trust value which is portrait of reliability is used with the link information to make a successful transmission. This scheme is further incorporated with interference model, in each time step. Being known the jammers parameters and channel state information, the information theoretic approaches can establish reliable communication and data confidentiality. Cardinality of the link is also considered for the learning purpose. The learned dynamics of the network is used to give a transmission path for guaranteed communication under secure environment.*

**Index Terms** - *MANETs, Trust Management, Channel Uncertainty, Jamming, Defensive measures, Anti-jamming.*

## I. INTRODUCTION

MANETs have become important communication key in environments where risks to the security needs to be considered seriously due to the distinctive feature of MANETs, which includes open wireless medium, distributed nature. A fundamental algorithmic challenge in the optimization of wireless communication is to maximize the number of simultaneous successful transmissions [1] [2]. However, in practice the network conditions can change dramatically in the presence of co-existing networks using different protocols or even maliciously behaving wireless transmitters. MANET technology has been evolving to use wider channel bandwidths over a very large channels and they support lower receiver sensitivity for a wider range. Also, Information theoretic approaches establish reliable communication and data confidentiality directly at the physical layer of a communication network by taking the properties of the noisy channel into account [2].

Nodes use timeslot to communicate which need high-precision time synchronization. Uncertain reasoning and trust management schemes, which originates from Artificial Intelligence community, can mitigate these security issues. Uncertain reasoning was used to solve problems in expert systems and also be used to derive Trust values for the node in the MANET. A common way to take these effects into consideration is by modeling interference conditions as if determined by an adversary, adapting to the algorithm's efforts over time [3]. Because frequency bands for MANET are already congested the wireless environment may suffer severe interference from unintentional jammers and intentional jammers and the failure probability of packet transmissions is expected to increase due to interference from other devices and jammers. Malevolent adversaries jam the channel of the legitimate users due to the open nature of the wireless medium [4]. Transmitted signals are received not only by the intended users but also are easily eavesdropped upon by non-legitimate receivers. The definition of trust in MANETs is similar to the explanation in sociology, where trust is interpreted as degrees of the belief that a node in a network [5].

In this paper, a new approach towards the identification and prevention of nodes is explored. Trust is considered as the reliability factor and cardinality is considered as link usages advantage. Considering the dynamic nature of the MANET, uncertainty is simulated using the channel state information and learned by a dataset encouraged by machine learning approach. Interference model is another security level in the proposed methodology which is helpful for generating noisy channel in order to secure the message under channel uncertainty. Learning dataset keeps track of changing environment and used these changes for more optimized outcomes. This network structure is also associated with the security measures such as defense methods and maximum cardinality ratio. Defense mechanisms include, fingerprint pre-distortion of device, allocation of dynamic ID for every joining and removal in the network and friendly jamming which can be used in preventing eavesdropper from getting any information in message transit. The decision for the usages of the greedy approach and/or security methods is done by learning dataset in the proposed scheme.

## II. BACKGROUND

Trust management scheme for security enhancement in MANET is proposed in [1]. Trust management scheme uses direct and indirect observation for derivation of Trust Values. Detection-based approaches use two important components: direct observations and indirect observations, for trust model. With direct observation from an observer node, the trust value is derived using Bayesian inference. On the other hand, with indirect observation from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory (DST).A distributed algorithm with adversarial jamming to extend the problem of capacity maximization is proposed in [2]. Links iteratively adapt their behavior to maximize the capacity of the single time steps. A very powerful adversary model of a bounded jammer is allowed to make all transmissions unsuccessful during a fraction of any time window of time steps. Beyond such a worst-case scenario, a stochastic jammer that blocks each time step independently at random with probability is addressed. Algorithms and their no-regret property can be used to obtain provable approximation factors for capacity maximization under adversarial jamming. In [3], persistent jamming attacks are discussed with the possible defense techniques. Defenses against these attacks comprise a digital fingerprint pre-distortion, dynamic ID allocation and dual channel friendly jamming. All these methods are also effective against adversarial jamming and can be associated with trust management scheme. In the proposed method of [4] different models for secure communication under channel uncertainty and adversarial attacks is given. It reviews the corresponding secrecy capacity, which characterize the maximum rate at which information can be sent to legitimate receivers while being kept perfectly security from eavesdroppers. This is done using the relevant Channel State Information (CSI) and is determined by compound channel realization. Secure single-hop pair-wise time synchronization is proposed in [5] which uses authentication and integrity methods to prevent external attacks and pulse-delay attacks. A secure cluster-wise time synchronization which improves µTESLA broadcast authentication mechanism is also proposed.

This paper presents brief introduction of Security architectures within ad-hoc network in Section I. Preliminary information is discussed in Section II, as Background. Section III discusses the previous work done. Section IV gives proper information about the existing methodologies. Section V discusses analysis of methodologies and gives advantages as well as disadvantages. Section VI gives proposed methodology on enhancement of security with trust management. Section VII briefs possible outcomes and results of the proposed methodology. Section VIII gives conclusion of the paper and Finally Section IX contains future scope for the current methodology.

## III. PREVIOUS WORK DONE

Zhexiong Wei *et al.* (2014) [1] proposed trust management scheme to enhance security in MANET. It has two components: Trust from Direct observations and Trust from Indirect observations. Bayesian interference and Dempster-Shafer theory is used in these components respectively. Trust is interpreted as the degree of belief that a node performs as expected. It recognizes uncertainty in trust evaluation. The elasticity and flexibility of uncertain reasoning make it successful in many fields, such as expert systems, multi-agent systems, and data fusion.

Johannes Dams et al. (2016) [2] proposed capacity maximization under interference conditions with a distributed algorithm. Nodes adopt the dynamic conditions of the network and against adversary model which is able to make all transmission unsuccessful during a fraction of time step. In particular, the number of successful transmissions becomes at least some fraction of the maximum number of transmissions that would have been possible in hindsight. By identifying several key parameters of the sequences of transmission attempts resulting from algorithms, no-regret learning algorithms adjust to compute such sequences with suitable values for the key parameters.

Ll-Gu Lee et al. (2016) [3] proposed a new jamming attack called persistent jamming and defense techniques against it. Attack is enabled by using partial ID used to save the power and device fingerprints in wireless network. In the defense, a digital fingerprint pre-distortion, dynamic ID allocation and friendly jamming is incorporated for anti-tracking and anti-jamming. The focus is on a realistic environment, i.e. a dense network, in which there are multiple devices using different channels.

Rafael F. Schaefer et al. (2015) [4] proposed Information theoretic approach which surveys different models for secure communications under channel uncertainty and reviews secrecy capacity. Channel state Information is idealized for communication conditions and allows obtaining an understanding and important insights of the fundamental principles of information theoretic security. It can also be used to determine the maximum rate at which information can be sent over a secure communication.

Wei Yang et al. (2016) [5] proposed secure time synchronization with a secure single-hop pair-wise and cluster wise approach. Message integrity authentication approach is adopted to defend against eternal attacks and pulse-delay attacks. This scheme can successful defend against time synchronization attacks as well as low energy consumption. The secure cluster-wise time synchronization adopts packet-based key chain to improve authentication mechanism which can well balance the delay of disclosed keys and the length of key chain.

## IV. EXISTING METHODOLOGY

### A. Trust Management Scheme

The trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory (DST), which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method. This trust value can be used to determine the usefulness of the node in network. In the derived method, secure routing is possible with trusted nodes where trust value yields maximum [1].

Trust from Direct Observation each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviors of the observed node. Therefore, the observer node can calculate trust values of its neighbors by using Bayesian inference. The trust from direct observation between an observer node A and an observed node B in this trust scheme can be defined as

$$T_{AB}^{S} = \rho T_{AB}^{D} + (1-\rho) T_{AB}^{C}$$

where $\rho$ ($0 \leq \rho \leq 1$) is the weight for data packets, $T_{AB}^{D}$ is the trust value based on data packets, and $T_{AB}^{C}$ is the trust value based on control packets

### B. Capacity Maximization under Interference Model

Overall goal of capacity maximization is to maximize the total number of successful transmissions over time. Success is defined using Interference Model, a framework based on edge-weighted conflict graphs that encompasses a variety of interference models, including the SINR model or models based on bounded-independence graphs like unit-disk graphs. Set of links is called *feasible* if all links in this set can successfully transmit simultaneously [2].

The network consisting of a set of wireless links $\boldsymbol{l_v = (s_v, r_v)}$ for $\boldsymbol{v \in V}$ composed of sender $s_v$ and receiver $r_v$. Overall goal of capacity maximization is to maximize the total number of successful transmissions over time. Success is defined using Interference Model, a framework based on edge-weighted conflict graphs that encompasses a variety of interference models, including the SINR model or models based on bounded-independence graphs like unit-disk graphs. Set of links is called feasible if all links in this set can successfully transmit simultaneously

### C. Defensive Techniques against jamming attack

A new jamming attack called ―persistent jamming is a modified reactive jamming that is effective in dense networks. The persistent jamming attack can track a device that switches channels using the following two features, partial association ID and fingerprint detection. Three defense mechanisms for anti-tracking and anti-jamming are used viz., a digital fingerprints pre-distortion, dynamic ID allocation, and dual channel friendly jamming. An attacker is able to extract and analyze the physical characteristics from the PHY header, such as timing offset, RSSI, signal-to-noise ratio (SNR), and error vector magnitude (EVM); then, it can track and jam a target device using the fingerprints. So, fingerprint pre-distortion is useful in countermeasures. Partial Associated ID in the signal field can be used to identify the destination of the packet for any node in the wireless network. Hence, dynamic ID allocation is needed. The dual channel friendly jamming scheme uses separate frequency channels as a legitimate transmitter and a friendly jammer in a time-division duplexing manner [3].

In this experiment, two defense combination cases are examined;

1) 'PJ defense without FJ under PJA' : Case employs digital fingerprints distortion and dynamic ID allocation mechanism without friendly jamming (FJ)
2) 'PJ defense with FJ under PJA' : Case performs digital fingerprints distortion and dynamic ID allocation with the dual channel friendly jamming.

### D. Information theoretic approach for uncertainty

The concepts explained are suitable for model secure communication in the presence of active adversaries and their potential attacks on the communication. Attacks are perfectly modeled by compound wiretap channels. Accordingly, AVWCs would then model even more powerful adversaries, whose jamming strategies change with time. A single transmitter-receiver pair in the presence of one external eavesdropper is the simplest model of secure communication. There has been some effort to extend the previously discussed concepts to more complex multi-user scenarios as well. Most noteworthy in this context is the broadcast channel with confidential messages. Similar to the wiretap channel, the sender transmits a confidential message to a legitimate receiver while keeping an eavesdropper ignorant. Additionally, the sender transmits a common message as well which is intended for both the legitimate receiver and the eavesdropper [4].

The ideal assumption of perfect CSI at all users and present the basic ideas and concepts of secure communication over such a wiretap channel. An $(n,M_n)$-code C for the wiretap channel consists of one stochastic encoder at the transmitter i.e., a stochastic matrix, with a set of confidential messages $M = \{1,. .\ ., M_n\}$.

$$E : M \rightarrow P(X^n)$$

and a deterministic decoder at the legitimate receiver

$$\varphi : Y^n \rightarrow M$$

The secrecy criterion ensures that the non-legitimate eavesdropper is not able to infer any information about the transmitted message. Let M be a random variable uniformly distributed over the set of messages M and $Z^n = (Z_1, Z_2, \ldots, Zn)$ be the channel output at the eavesdropper. The secrecy of the confidential message in terms of equivocation having in mind that the channel output at the eavesdropper $Z^n$ should not reveal any information about the message

### *E. Secure time synchronization for security*

It offers both message encryption service and message integration check services. Message encryption uses Electronic Code Book (ECB) mode to encrypt message and message integration authentication computes message encryption code (MIC) in Cipher Block Chaining (CBC) mode. The core encryption method used is 128-bit AES. A sender and receiver have to set the 128-bit key at the beginning. Then the sender generates the MIC for both pair-wise and cluster-wise time synchronization messages in the MAC layer. In the process of pair-wise time synchronization, the receiver can computer the MIC used the secret key shared with the sender once it receives the time synchronization message. In the process of cluster-wise time synchronization, the receiver has to buffer the arriving time synchronization message until it receives the disclosure of keys [5].

Two types of time synchronization attacks: by modifying the value of *TsTx* offset in the timeslot template, which it call the timeslot template attack and by delaying the transmission of the time synchronization packet, which it call the pulse-delay attack.

Let T1 and T2 represent the record time of transmitter, and R1 and R2 represent the record time of receiver in the process of single-hop pair-wise time synchronization.

$$A \rightarrow B: A, B, T1, N_A, MAC(K_{AB}, A, B, T1, N_A)$$

$$B \rightarrow A: B, A, T1, R1, R2, N_A, ACK,$$

$$MAC(K_{AB}, B, A, R1, R2, N_A, ACK)$$

$$offset = \frac{(R1 - T1) - (T2 - R2)}{2}$$

$$dealy = \frac{(R1 - T1) + (T2 - R2)}{2}$$

## V. ANALYSIS AND DISCUSSION

Nodes in the network are a fundamental for communication, so it must be reliable mandatorily. Trust value determines this property of the node and usability is calculated. To calculate trust value, Bayesian interference methods as well as Dempster-Shafer methods are used. These methods are basically used in the direct and indirect ways. Direct methods consider neighboring nodes with reliable trust value and indirect methods considers observation from neighboring nodes. There are two algorithms for these observations. While trust value is being calculated, average end-to-end delay is increased. Since the metric link value is introduced in the MANET, message overhead is also increased [1].

Successful transmission of messages is a basic necessity for the communication; hence number of successful transmission must be increased relatively. However, in practice the environment can change rapidly, particularly in the presence of co-existing networks using different protocols or even maliciously behaving wireless transmitters. Interference model is introduced for this purpose. But interference model not only affects the malevolent nodes but also affects the transmission between the legitimate users. This interference model is able to make all transmission unsuccessful during the fraction of the time step. Learning the network dynamics and its changes is one way to resist the interference. Large scale sensor networks or ad-hoc networks giving such information to links can be infeasible [2].

Proactive jammers are not effective in the dense network but reactive jamming can be 80% effective in the dense network. The new jamming attack, persistent jamming, is one of reactive jammers. Defense mechanism against persistent jamming consists of three methods; fingerprint pre-distortion, dynamic ID allocation and friendly jamming. All these methods provides security in the dense network with some drawbacks such as, the ID detection success ratio was higher than 90% for all locations, and the fingerprint detection success ratio was higher than 80% for all locations. If there is no neighboring node, defense performance is poor because persistent jammer does not have another choice [3].

**Table 1: Comparison between existing methodologies**

| Security Techniques | Advantages | Disadvantages |
|---|---|---|
| Trust Management Scheme | 1) The proposed scheme has much higher PDR than the existing scheme because the trust-based routing calculation can detect the misbehavior of malicious nodes.<br>2) Throughput of the network has significant increase when trust-based routing algorithms are used. | 1) Security enhancement in OLSRv2 also increases the average end-to-end delay.<br>2) Since the metric link value is introduced in MANET, message overhead is increased. |

| | | |
|---|---|---|
| Capacity Maximization under interference model | 1) The algorithms are based on no-regret learning techniques to exploit the non-jammed time steps as efficiently as possible.<br>2) All links can successfully transmit simultaneously in SINR interference model achieving capacity maximization. | 1) In practice the environment can change rapidly, particularly in the presence of co-existing networks using different protocols or even maliciously behaving wireless transmitters.<br>2) Large scale sensor networks or ad-hoc networks giving such information to links can be infeasible. |
| Defensive techniques against jamming attack | 1) Digital fingerprints pre-distortion and dynamic ID allocation mechanisms are effective to prevent from device tracking and persistent jamming attack.<br>2) If there is at least one legitimate node, the digital pre-distortion and dynamic ID allocation can mitigate the effect of the persistent jamming attack. | 1) Persistent jamming can improve the attack efficiency by approximately 80% in dense networks compared with reactive jamming schemes.<br>2) If there is no neighboring node, defense performance is poor because persistent jammer does not have another choice. |
| Information theoretic approach for uncertainty | 1) An informed transmitter usually leads to an increase in secrecy capacity this allows the transmitter to adapt the encoder according to the particular transmission.<br>2) In Compound wiretap channel, small variations in the uncertainty result only in small variations in the secrecy capacity. | 1) A drawback of this approach is that it relies on the assumption of insufficient computational capabilities of non-legitimate receivers resulting in so-called conditional security.<br>2) In practical systems CSI will always be limited due to the nature of the wireless medium and estimation/feedback inaccuracy. |
| Secure time synchronization for security | 1) Highly reliable and ultra-low power.<br>2) High precession time synchronization. | 1) Single Communication channel in MAC layer. |

## V. PROPOSED METHODOLOGY

MANET consisting dynamic nature of network structure needs a more sophisticated approach for the identification of nodes and prevention of the malevolent behavior of jammers and/or attackers. We focus on this requirement by introducing a new approach towards node identification and eavesdropper detection and prevention using learning methods which uses some existing with newly proposed methods. Trust values are already been described earlier which gives the usefulness of the node and its reliability. Based on the definition and properties of trust in MANETs, Trust in the proposed scheme is evaluated by a real number $T$ with a continuous value between 0 and 1. In this model, trust is made up of two components: direct observation trust and indirect observation trust. A trust value from direct observation can be denoted as $T^S$ and can be calculated by Bayesian inference. The trust value derived from indirect observation of one-hop neighbors can be denoted as $T^N$. Combining the trust value $T^S$ from direct observation and the trust value $T^S$ from indirect observation, we can get a more realistic and accurate trust value of a node in MANETs,

$$T = \lambda T^S + (1-\lambda)T^N \quad \text{.....(1)}$$

where $\lambda$, $0 \leq \lambda \leq 1$ is a weight assigned to $T^S$.

In the direct observation, we assume that each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviors of the observed node. Therefore, the observer node can calculate trust values of its neighbors by using Bayesian inference. In the indirect observation, the Dempster-Shafer Theory is used as it is well developed for coping with uncertainty or ignorance, and it provides a numerical measurement of degrees of belief about a proposition from multiple sources. Node $N$ information consist of {*NID, T*} node ID and Trust value associated with it.

The performance of capacity maximization algorithms with adversarial jamming is also modeled here. A central idea in construction is to divide time into phases. Here, a *phase* refers to a consecutive interval of time steps. The set of phases $R_v$ for link $l_v$ do not require the phases of different links to be synchronized. A phase is labeled as either successful or unsuccessful. It is *successful,* if link attempts transmission throughout the phase and at least a fraction of time steps within the phase. If

transmission for link $l_v$ is successful for all of its receivers that are conflict-free, maximum transmissions of links reach their receivers. If transmission for link $l_v$ is successful for at least one receiver which is a conflict-free, transmission are maximum for at least one of their receivers. If utility of a link is linear in the number of receivers that are conflict-free, the number of successful transmissions at the receivers is maximum. No-regret learning can use these sets for developing a dataset called *cardinality* to give a reliable route to the destination for successful transmission. Cardinality $C$ can consist of $\{ R_v , l_v \}$ set in its table format, which is time step and link set which guarantees reliable transmission. The learning dataset $M$ consist of $\{C, N\}$ cardinality and node pair which can give a best option for the successful transmission of data packets.

Above explanation only gives the reliable communication links as well as nodes, now we focus on the security of theses link-node transmission scheme. There are three basic defense techniques proposed here, particularly against the jamming attack. The proposed scheme is defense to successfully protect fingerprints and ID from jamming attack which is evaluated based network emulation methodology. Throughput is calculated by dividing the length of a successfully transmitted packet by the time $t$ taken to transmit the packet. Therefore, overhead time other than the time that the packet occupies a channel should be reduced to increase the throughput. If there is at least one legitimate node, the digital pre-distortion and dynamic ID allocation can mitigate the effect of the jamming attack. On the other hand, if there is no neighboring node, defense performance is poor. It is difficult for an attacker to track the device fingerprints because the periodically changed offsets and signal quality due to the digital pre-distortion scheme are hidden from others. These methods yields the channel between sender and receiver which can give maximum value for cardinality set as well as trust value which can be shown as follows.

Algorithm above takes input as a set of nodes and links between them, and progress towards finding the most reliable link-node pair for successful transmission. Trust values and Cardinalities are calculated for nodes and links respectively. These values determine the reliability of each and can be used by attackers and jammers also. Interference model initialized to protect the transmission of message over the uncertain link. This interference model is designed in order to create noisy channel for eavesdropper or jammer and makes legitimate channel transmission easy as compared to attack. Then comes the learning dataset, which is of the form Cardinality – Node association can be used to decide whether to use defense methods or greedy approach or both or go for the transmission directly.

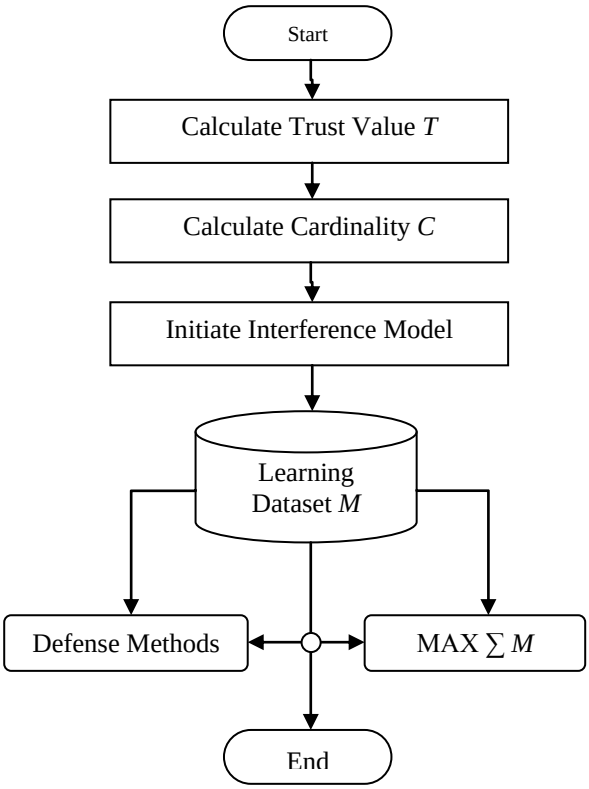


**Fig. 1: Flowchart for the Defensive & learning scheme.**

This dataset stores the information according to the history of the network and outputs the most used and trusted nodes and most reliable links to those nodes. In defense methods, fingerprint pre-distortion, dynamic ID allocation and friendly jamming is used. In greedy approach, maximum of dataset $M$ is used.

## VI. POSSIBLE OUTCOMES AND RESULT

In the presented paper, the effectiveness of the scheme is evaluated in an insecure environment. The trust-based node selection can improve the performance. The results demonstrate that the proposed scheme with indirect observation has the highest response for trust value calculation. Proposed scheme based on trust outperforms the existing scheme significantly in terms of efficiency and throughput. Since the Cardinality value is introduced in MANET, message overhead is decreased. Proposed approach yields a good convergence towards the optimum. It is especially promising that the constant factors used in our analysis seem to be negligible. The learning dataset considered is a variant of the Randomized Weighted Majority Graph Algorithm. Networks yields where interference from other nodes is the main reason for unsuccessful transmissions. The rapid changes in the environment can easily be learned and stored in the dataset which improves the processing efficiency. Large scale networks or ad-hoc networks giving such informative approach to links can be feasible. Jamming efficacy could be improved as jamming speed is faster.

Therefore, it is possible to detect the target node when the attacker switches for full channel scanning. If the proposed dual channel friendly jamming scheme is adopted, it can reduce the detection success ratio of the persistent jamming attack.

## VII. CONCLUSION

Using recent advances in uncertain reasoning, Bayesian inference, and DST, the trust values of observed nodes are evaluated in MANETs. Misbehaviors such as dropping or modifying packets can be detected in the scheme through trust values by direct and indirect observation. No-regret learning for capacity maximization with jamming is analyzed. These algorithms can be used to successfully tackle capacity maximization with jamming in both theory and simulations. Overall, the performance of no-regret learning remains robust in all cases. The effectiveness of the jamming schemes is evaluated and it demonstrates that jamming can attack target nodes in dense networks even though they adapt the channel frequency to avoid jamming signals. But pre-distortion of fingerprint of device and dynamic ID allocation can mitigate these effects. Information theoretic concepts that model secure communication under channel uncertainty.

## VIII.FUTURE SCOPE

In the future work, the proposed scheme will be expanded to MANETs with cognitive radios. Besides adversarial and stochastic jamming, it can successfully address further generalizations of the scenario with little overhead. Capacity maximization will be proved for large scale sensor networks. The persistent jamming attack for other wireless networks can be applied to test the extendibility of its efficacy and investigate more efficient defense mechanisms against persistent jamming attacks in terms of complexity and defense performance. Another limitation of the wiretap channel will be overcome which is the simplest scenario involving one legitimate transmitter-receiver pair and one eavesdropper. As well as secure network-wide time synchronization for IEEE802.15.4e networks will be designed.

## ACKNOWLEDGMENT

I, Varad A. Sarve, am thankful of my supervisors Professor Dr. V. M. Thakare and Professor Dr. S. S. Sherekar for helping to complete this research paper.

## REFERENCES

[1] Zhexiong Wei, Helen Tang, Richard Yu, Maoyu Wang, Peter Mason, "Security Enhancement for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE transaction on Vehicular Technology, Vol. 63, No. 9, Pg. No. 4647-4658, September 2014.

[2] Johannes Dams, Martin Hoefer, Thomas Kesselheim, "Jamming-Resisten Learning in Wirelss Networks", IEEE transaction on Networking, Vol. 24, No. 5, Pg. No. 2809-2818, October 2016.

[3] Li-Gu, Myungchul Kim, "Persistent Jamming in Wireless Local Area Networks: Attack and Defense", 10.1016/j.comnet.2016.06.024, June 2016.

[4] Rafael F. Schaefer, Holger Boche, H. Vincent Poor, "Secure Communication Under Channel Uncertainty and Adversarial Attacks", Vol. 103, No. 10, Pg. No. 1796-1813, October 2015.

[5] Wei Yang, Jie He, Ruijie Zhang, Qin Wang, "STS_4e: Secure Time Synchronization in IEEE802.15.4e Networks", 10.1007/s10776-016-0322-3, September 2016.