TRUSTED AND LIGHTWEIGHT DYNAMIC SOURCE ROUTING (TL-DSR) PROTOCOL TO WITHSTAND AGAINST SELFISH ATTACK IN MOBILE AD HOC NETWORKS BASED MILITARY ENVIRONMENT

K. Prathapchandran[1]

Abstract

Securing MANET based military environment is always a challenging task because of various security threats in the form of attacks. Among the threads, selfish behavior is one of the considerable issues in recent research because it is not launched from outside the network instead they launched from inside of the network by compromised nodes. The main objective of selfish nodes is not to involve in any network related operations so as to save their energy by the way they try serve in the network for a long time. Hence, the performance of the mission will reduce. In this paper, a Trusted and Lightweight Dynamic Source Routing (TL-DSR) protocol to withstand against Selfish soldier/nodes in MANET based military environment is proposed. The main objective of this paper is to ensure authentication by identifying selfish soldiers/nodes based on the Overall Rating (OR) which is calculated based on the soldiers' Interaction Rating (IR), Packet Forwarding Rating (PFR), Social Rating (SR) such as attitude, behavior, belief, honest and responsibility of soldiers. The proposed mechanism does not involve with any complex algorithm instead of we make use of lightweight mechanisms in the form of trusts. In order to evaluate the proposed mechanism, simulation tool is used. The simulation results shows that the proposed mechanism is better than standard DSR and existing approach that similar to the proposed one.

Keywords : Mobile Ad hoc Networks, Military, Security, Trust, Selfish behavior, Interaction Rating, Packet Forward Rating and Social Rating.

I. Introduction

Mobile Ad hoc Networks also known as MANET is a collection of autonomous mobile nodes that are connected together over an open and shared wireless medium. Nodes in the networks are moving freely so the topology of network is always changing. Like traditional network there is no dedicated router for forwarding the packets instead of that each node acts as router for forwarding the packets (Sivagurunathan et al, 2015). These types of networks are launched without any aid of fixed infrastructure and it can be setup on demand. Because of the special features, it leads to various applications such as emergency, healthcare, rescues, military and etc. Among the applications, military is one of considerable application that deployed in MANET. The reason is, setting up of fixed access point and backbone infrastructure is not always possible because infrastructure may not practical for military application. In addition, infrastructure may not present for short range radios. Hence, the MANET is best suitable for military environment.

[1] Assistant Professor, Department of Computer Applications, Karpagam Academy of Higher Education, Karpagam University Coimbatore, India. E-mail : kprathapchandran@gmail.com

Success of any application depends on how it is secured (Sivagurunathan et al, 2016). Therefore enhancing security is one the considerable research in MANET based military environment because it is always having confidential information hence passing of information from one soldier to another should be carried out efficiently means without any loss and on time then only the objective of the mission can be achieved. MANET itself has a security issues and in addition as military environment is deployed in it, the security is getting highly attention among the researchers. Achieving security is always a challenging task because security threads in MANET deployed military environment is coming in the form of various attacks. Among the attacks selfish behavior is one of the considerable and most dangerous attacks because this kind of attack is launched internally from compromised nodes. The aim of the selfish behaviors [Annadurai et al, 2015] is not to forward the packets to others nodes by the way they try to save their battery power. Hence, they simply refuse the incoming packets.

The rest of the paper is organized as follows; section 2 discusses the review of literature, section 3 discusses the proposed technique called Trusted and Lightweight Dynamic Source Routing (TL-DSR) protocol, section 4 discusses the simulation results and finally section 5 concludes the paper.

II. Review of Literature

The following section discusses the existing techniques. Islam et al, 2014 proposed an agent based on demand routing protocol to avoid selfish behavior. This work follows the selective forwarding technique to identify selfish behavior. The main purpose is to manage trust information locally with minimal Overhead in terms of extra messages and time delay within the network. Tameem et al, 2011 proposed a trust based routing mechanism which is based on friendship mechanism. The selected node will follows the features such as node reputation and identity information before forwarding the data packets. CAST: Context-Aware Security and Trust framework for Mobile Ad-hoc Networks using policies proposed by wenjia et al., 2012. The main aim of this paper is to identify the malicious node based on the contextual information such as communication channel status, battery status, and weather condition. Hui Xia et al, 2016 proposed a trust enhancement framework which is based on the historical trust assessment and trust prediction. In this approach a dynamic grey-Markov chain prediction is used for prediction. In addition the authors Priya et al, 2015, Jamal et al, 2008, Nadia et al, 2014 and P. Annadurai et al, 2015 proposed mechanisms to withstand against selfish attack based on trust mechanisms.

III. Proposed Work : Trusted and Lightweight Dynamic Source Routing (TL - DSR) Protocol

3.1 Assumptions for the proposed work

- At the time of initial network/mission deployment, all the soldiers/nodes are authenticated; having well defined resources and the energy level is high.

- Every soldier is capable to calculate the trust value of other soldiers and not by own.
- The various trust calculations and Overall Rating (OR) lies between 0 to 1
- Neither source soldier nor destination soldier can be a selfish
- Neighbors list are created among the soldiers at the initial mission deployment
- Number of selfish soldiers always less than the good soldiers
- Every soldier maintains a trust table where trust related information is stored. The underplaying structure of the trust table is shown in the table 1.

Table 1. Soldier's Trust table

SID	IR	PFR	SR	OR	DT	D

SID- Soldier's IdentityIR- Interaction Rating, PFR-Packet Forward Rating, SR-Social Rating,DT-Decision Trust and Decision-D

- As every soldiers/node is in promiscuous mode, they can able to know the packet forwarding status, past interactions of other soldiers and personal attributes as well. Soldiers' promiscuous mode structure is depicted in the figure 2.

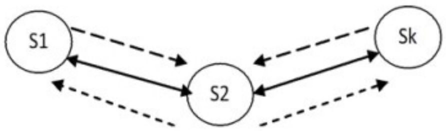

Figure 1 . Representation of soldier's promiscuous mode

In the above figure S1, S2 and Sk represents the soldiers. When S1wants to forward certain number of packets to Sk through S2, in this case S1 records packet entries in its buffer and monitors whether S2 has forwarded all the packets to Sk. Because of promiscuous mode, Sk overhears packets received by S2 maintains its buffer.

The proposed TL-DSR protocol consists of the following phases :

- Trust evaluation phase
- Identification of selfish soldiers

3.2 Trust evaluation phase

As mentioned in the assumption, initially all the soldiers are trustworthy. Over the period of time the soldier may behave as selfish result in overall performance degradation in mission activity. Hence, every soldier is in situation to identify the selfish soldiers by executing the TEL-DSR so that authentication of the each soldier can be ensured. Trust evaluation phase involved with various trust calculation such as soldiers' Interaction Rating (IR), Packet Forwarding Rating (PFR) in terms of network functionalities, soldier's Social Trust (SR) in term of their personal behavior and soldier's node energy. In Military environment, soldiers may carry the communication equipments with them or automated military vehicles may communicate with other vehicles without human interventions. Hence, military environment is depends on three types of communication such as node to node communication, node to human or human to node communication and human to human communication. To achieve effective communication among the soldiers, these three communications are essential. As military environment is highly sensitive, weakness in any of these communication will make trouble in overall mission performance. Therefore, we consider all these communication in evaluating trust worthiness. Node to node communication is accomplished by networking devices whereas human to human communication is accomplished by in person while they are talking. In addition, node to human or human to node communication accomplished when a soldier wants to communicate with other soldier by using their military communication equipments. Typically, it is done in the soldier itself so we are not considering this communication. As mentioned earlier, the proposed mechanism is involved with three types of trust evaluation such as Interaction Rating (IR), Packet forwarding Rating (PFR) and Soldier's Personal attributes or characters Rating (PAR). The first two rating are calculated based on node to node or human to human communications and last rating is only based on the human to human interaction means soldier to soldier communication.

3.2.1Interactions Rating (IR) calculation

We adopt the graph theory in order to evaluate the IR. In this proposed approach, military environment has been represented as a directed graph G(V,E) where V is set of vertices representing participating soldiers/nodes in the mission and E is a set of edges representing interaction among the participating soldiers. Each edge has a weight that denoting the number of interaction initiated and carried out by a soldier with other soldiers in order to execute the mission. As military environment is assumed as directed graph, the edge of a graph may have in degree and out degree. The in-degree denotes the number of soldiers interacting with the selected soldier and out-degree denotes a soldier is interacting with many soldiers. The figure 2, depicts the MANET based military environment is depicted as a directed graph. The interacting rating is calculated based on the in-degree and out-degree of the soldiers.

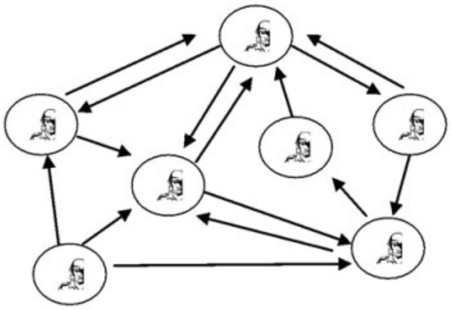

Figure 2. MANET based military Environment is represented as a directed graph.

Table 2 : Interaction Rating for in degree and out degree

In-degree	Out-degree	Rating
High	High	1
High	Low	0.5
Low	High	0.5
Low	Low	0

A soldier has high out-degree means he/she is actively participating in mission related activities by propagate the information to other soldiers during the execution of the mission. High in-degree means he /she is actively responding the soldier's generated request so that more number of soldiers are interacting with him/her so as to execute the mission.

A solider has low out degree means he/she propagates less mission related information to others because he/she may not have interest in participating in mission related activities or he/she may be in trouble. Low in degree means a soldiers receives less mission related information from other soldiers because he/she may not actively participating in the mission related activities so other soldiers might not request a query that related to missions. The determination of in-degree and out-degree is set based on the pre –determined threshold value that is depicted in the following equation 1.

$$\begin{array}{c} If\ in-degree >= threshold, High \\ If\ out-degree > = threshold, High \\ If\ in-degree < threshold, low \\ If\ out-degree < threshold, low \end{array} \quad (1)$$

Based on the equation 1, the table 2 is formulated and it is providing rating for both in-degree and out-degree. Hence, we conclude that both in-degree and out-degree determines the interaction capabilities of the participating soldiers. Then based on the interaction we can assign rating. If both in-degree and out-degree of the soldier's high means we assign the IR as 1. If both in-degree and out-degree of the soldier's low means we assign the IR as 0. If in-degree is high and out-degree is low means and also vice versa means we assign as 0.5.

3.2.2 Forwarding Rating (FR) Calculation

Then each soldier calculates the PFR based on the number of packets he or she is transmitted. The reason behind this calculation, sometimes interaction is not enough to evaluate the trustworthiness of the soldiers because however a soldier may have high number of out-degree and in-degree, when transmit the packets to other soldiers due to the distinct characteristics of MANET, the packets may not reach the destination as it transmits there is a possibility of packet loss. This shows mission related information may not reach fully. Hence, poor performance in overall mission objective. To overcome such issue, we consider packet forwarding rating as one of the metric in evaluating trustworthiness of the soldiers. The packet forwarding rating is calculated based on the following equation 2. Soldier Si evaluate the packet forwarding ratio of soldier Sj over the period t based on direct observations of packet forwarding ratio. It can be represented as, At time t_1,

$$FR_{ij}^{D}(\mathrm{t}) = \frac{NCF_j - NCD_j}{NCP_j} + \frac{NDF_j - NDD_j}{NDP_j} \qquad (2)]$$

In the eq.2, $FR_{ij}^{D}(\mathrm{t})$ denotes forwarding ratio of soldier j evaluated by soldier i at t, similarly, NCF_j denotes the number of control packet forwarding ratio of soldier j, NCD_jdenotes the number control packet dropping ratio of soldier j,NDF_j denotes number of data packet forwarding ratio of soldier j andNDD_j denotes number of data packet dropping ratio of soldier j. The cumulative PFR is finally calculated to assign Rating. The following equation 3 depicts the Rating for the cumulative packet forwarding.

$$\begin{array}{c} If\ cumulative\ PFR > Threshold, \quad Rating = 1 \\ If\ cumulative\ PFR < Threshold, \quad Rating = 0 \\ If\ cumulative\ PFR = Threshold, \quad Rating = 0.5 \end{array} \quad (3)$$

3.2.3 Social Rating (SR)

The objective of considering this factor is, a soldier may have high IR and PFR, but he/she may not good at social perceptive at the time of mission execution. For instance, generally family commitments and problems will affect everyone in their workplace. Therefore, if soldier has family problem and other issue, he may not involve in mission related activities hence performance degradation in overall mission objective. So we consider the social rating as one of the factor in evaluating trustworthiness. In this proposed work, we consider soldier's attitude, behavior, belief, honesty and responsibility factors to determine the social rating of the soldiers. The table 3 depicts the various personal attributes and corresponding rating.

Table 3. Personal attributes and corresponding rating of soldiers

Various Personal Attributes					
Attitude	Behavior	Belief	Honesty	Responsibility	Rating
Negative Attitude	Wrong Behavior	Dissimilar beliefs	Dishonest	Irresponsible	0
Marginally Positive Attitude	Marginally good Behavior	Marginally similar beliefs	Marginally honest	Marginally responsible	0.5
Positive Attitude	Good Behavior	Similar beliefs	Honest	Responsible	1

Attitude of the soldier refers the image created in a soldier's mind about the psychological state of another soldier. Psychological state nothing but the feelings, values, mood, and disposition of soldiers during the execution of the mission. Next, behavior represents an action and reaction of a soldier under a critical circumstance of military environment. Beliefs represent the confidence of the soldier in executing the mission or a particular mission related task. Responsibility refers whether a soldier is responsible with respect to all queries that are generated by other soldiers towards to the execution of the mission. Finally, honesty represents whether a soldier is behave like a fraudulent or not with respect to mission related activities. Based on the attributes, social rating of a soldier is calculated. The following table 4 depicts the various attributes rating of various soldiers evaluated by soldier1.

After evaluating the soldier's personal attributes, overall social rating of particular soldier is calculated. That is calculated based on the following equation

$$\begin{array}{c} \textit{If maximum attributes gives negative values,} \\ \textit{we assign Social Trust} = 0 \\ \textit{If marginal or same number of negative/positive values, we assign social rating} = 0.5 \\ \textit{If maximum attributes gives positive values,} \\ \textit{we assign social rating} = 1 \end{array} \quad (4)$$

Table 4. Soldier 1's interaction wise social rating of other soldiers based on the five attributes

SId	No.of Interactions	Attributes				
		Attitude	Behavior	Belief	Honesty	Responsibility
S_2	7	0, 1,1,1,0.5,0.5,1	1,1,1,1,0,0,0.5	0.5,1,1,1,1,0.5,0.5	0,0,1,1,1,0.5,0.5	0,0,0,0,1,1,1
S_3	4	1,1,0.5,0.5	0,0,1,1	1,1,0.5,0	0,0,1,1	0.5,0.5,0.5,1
S_4	6	1,1,1,1,0,0	0.5,0.5,1,1,1,0	0,0,0.5,0.5,1,1	1,1,1,1,0,0.5	0.5,0.5,0,0,1,1
S_5	5	0,0,1,1,1	0.5,0.5,1,1,1	0,0,1,1,1	0.5,0.5,0,0,0	1,1,1,0.5,1
S_6	9	0.5,0.5,1,1,11,0,0,1	0,0,0.5,1,1,1,0.5,0,0	1,1,1,1,0,0,0.5,0.5,1	0.5,0.5,1,0,1,0,1,1,1	1,1,0.5,1,0.5,0,0,1,1
S_7	2	1,1	1,1	0.5,0	0,0	1,1

Based on the above equations, the following table 5 has formulated. That is formulated by soldier1 for other soldiers.

After evaluating the attributes, each soldier will find the social rating of each soldiers based on the calculated above attributes. The following equation depicts the social rating calculation.

$$Social\ Rating\ (SR) = \mu1 * attitude + \mu2 * behavior + \mu3 * belief + \mu4 * honesty + \mu5 * Responsibility$$

$$Where, \mu1 + \mu2 + \mu3 + \mu4 + \mu5 = 1 \qquad (5)$$

After the evaluation of social trust, soldier will calculate the overall Rating of each soldiers based on the calculated social Rating (SR), Forward Rating (FR) and Interaction Rating (IR). The following depicts the Overall Rating (OR) of each soldiers calculated by Soldier.

$$Overall\ Rating\ (OR) = \mu1 * Interaction\ Rating + \mu2 * Forward\ Rating + \mu3 * Social\ Rating$$

$$Where, \mu1 + \mu2 + \mu3 = 1 \qquad (6)$$

Table 5. Soldier 1' overall rating of five attributes of other soldiers

Soldier's ID	No.of.Interactions	Attributes				
		Attitude	Behavior	Belief	Honesty	Responsibility
S_2	7	1	1	1	1	0
S_3	4	0.5	0.5	1	0.5	0.5
S_4	6	1	1	0.5	1	0.5
S_5	5	1	1	1	0	1
S_6	9	1	0.5	1	1	1
S_7	2	1	1	0.5	0	1

3.3 OR Propagation and Identifying Selfish nodes

Once the overall rating is calculated, based on the OR evaluating soldier will take decision on other soldiers based on the threshold table 6 which is shown in the table. If OR is greater than or equal to threshold value, those nodes become trusted nodes hence they will involve in route discover process. Otherwise they are untrusted nodes means selfish nodes. Information about the selfish nodes is broadcasted by every node to its neighboring nodes. Upon receiving, neighbor nodes delete the entries of untrusted nodes in its route cache. By the way authentication of Soldiers can be ensured.

Table 6. Decision Table

Level	DT	Decision
1	$OR \geq Threshold$	Authenticated Node
2	$OR < Threshold$	Untrusted node or Selfish node

IV. Simulation Results and Discussion

The proposed TL-DSR is implemented and tested in Network Simulator (NS3). The number of mobile nodes involved in the simulation is 75. Those nodes are placed randomly in 1000m x 1000m flat area. The total simulation run time is 500s. The DT value of each node calculated at regular interval of 200s over 600s. We have run the simulation for three times for each interval. We have chosen the source and destination node in random fashion with random way point mobility model.

The maximum speed of mobile node is set to 30m/s and minimum is set to1 m/s. the node pause is 0. The

IEEE 802.11b is used as the medium access control protocol. UDP-CBR (Constant Bit Rate) is used as a traffic generator. The packet size is 64 byte with the data rate of 3072bps. To analyze the impact of Selfish node node in the network, we have chosen randomly in increasing percentage. The proposed routing protocol is compared with standard DSR routing protocol and TDSR (Mohnapriya et al., 2013) routing protocol. To analyze the performance we used the following performance metrics such as packet delivery ratio and probability of detection for each metric, we increase the number of Selfish node nodes.

4.1 Packet Delivery Ratio Versus Percentage of Selfish node nodes

The figure 3 depicts the packet delivery ratio versus Selfish node nodes in percentage.

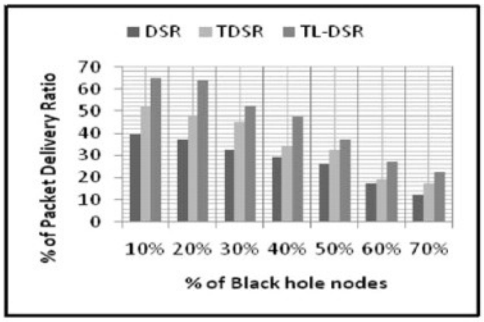

Figure 3. Packet delivery ratio

From the fig. 3 we observed that packet delivery ratio of TL-DSR remains high compared with DSR and TDSR though the number Selfish node nodes have increased. The reason is Selfish nodes are identified and isolated from the network based on the OR values before they involve in route discovery process. So route establishment is only involved with authenticated and trusted nodes therefore packet delivery ratio has increased though Selfish node nodes has increased. On the other hand in TDSR packet delivery ratio low compared with TL-DSR. The reason is evaluating trust worthiness focused only on packet forwarding ratio. Hence probability of Selfish node nodes remains high therefore packet delivery ratio is low. But in TL-DSR trust evaluation is based on multi factors so maximum effort has given to evaluate the trust worthiness. In standard DSR, as there is no detection mechanism of Selfish nodes by default, packets are dropped therefore packet delivery ratio degrades significantly whenever Selfish nodes increases.

4.2 Detection ratio versus percentage of Selfish node nodes

The following figure 4.represent the detection ratio of TDSR and TEL-DSR.

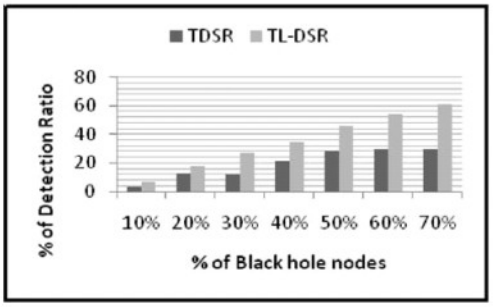

Figure 5. End to end delay

V. Conclusion

In this paper, Trusted and Lightweight Dynamic Source Routing (TL-DSR) protocol to withstand against Selfish attack in MANET based military environment is proposed. Here, the trust evaluation did not focus on complex cryptographic algorithms instead simple calculations such as Interaction Rating (IR), Packet forward Rating (PFR) and Social Rating (SR) are considered. Hence, the proposed TL-DSR is light weight therefore it is quite suitable for resource constrained military devices. Simulation results have proven that LT-DSR is given better results compared with standard DSR and TDSR.

References

1. Priya Sethuraman and N. Kannan, *"Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET",* Wireless Netw, DOI 10.1007/s11276-016-1284-1.

2. Jamal N, Al-Karaki, Ahmed and E. Kamal, *"Stimulating Node Cooperation in Mobile Ad hoc Networks",* Wireless Pers Commun (2008) 44:219–239.

3. Nadia Moati, Hadi Otrok, Azzam Mourad and Jean-Marc Robert, *"Reputation-Based Cooperative Detection Model of Selfish Nodes in Cluster-Based QoS-OLSR Protocol",* Wireless Pers Commun (2014) 75:1747–1768

4. P. Annadurai and S. Vijayalakshmi, *"Highly Reputed Authenticated Routing in MANET (HRARAN)",* Wireless Pers Commun (2015) 83:455–472

5. Islam Tharwat Abdel-Halim, Hossam Mahmoud Ahmed Fahmy and Ayman Mohammad Bahaa-Eldin, *"Agent-based trusted on-demand routing protocol for mobile ad-hoc networks",* Wireless Netw (2015) 21:467–483

6. Tameem Eissa, Shukor Abdul Razak, Rashid Hafeez Khokhar & Normalia Samian, *"Trust-Based Routing Mechanism in MANET: Design and Implementation Trust-Based Routing Mechanism in MANET: Design and Implementation"* (2013).

7. Wenjia Li , Anupam Joshi and Tim Fini, *"CAST: Context-Aware Security and Trust framework for Mobile Ad-hoc Networks using policies",* Distrib Parallel Databases (2013) 31:353–376

8. Hui Xia1, Jia Yu1, Zhen-kuan Pan1, Xiang-guo Cheng, Edwin H. -M. Sha, *"Applying trust enhancements to reactive routing protocols in mobile ad hoc networks",* Wireless Netw (2016) 22:2239–2257

9. S.Sivagurunathan and K.Prathapchandran, *"Trust based Security schemes in Self – Organized Networks (SON)",* Handbook of Research on Self-Organized Mobile Communication Technologies, IGI Global, pp.92-114, (2016).

10. S.Sivagurunathan and K.Prathapchandran, *"A Centralized Trust Computation model for secure group formation in Military based Mobile Ad hoc networks Using Stereotype",* Advances in Intelligent Systems and Computing, Springer, Vol.412, pp.427-438, (2015)

11. M. Mohanapriya , Ilango Krishnamurthi , *"Trust Based DSR Routing Protocol for Mitigating Cooperative Black Hole Attacks in Ad Hoc Networks "* Arab J Sci Eng (2014) 39:1825–1833 DOI 10.1007/s133 2001.