Context Attacks on CBSTM-IoT

Cody Lewis

February 11, 2020

We implemented a simulation of the trust model proposed in [2], this trust model managed to mitigate the context attacks.

1 Configurations of the Simulation

Our simulation contained 100 nodes where 30 were adversaries, that is, to show the effects of the attack while still below the Byzantine threshold [1]. Friendships between nodes was determined randomly such that the average amount of friends that each node had was approximately 50, then $frlow$ and $frhigh$ were calculated as a standard deviation below and above that mean respectively.

We defined the relationship factor with the following function,

$$R = \frac{1}{2^n} \tag{1}$$

where n is the degree of separation between nodes i and k. Where nodes belonging to the same owner have 0 degrees of separation, and those belonging to different owners have 1 degree of separation. Owners have at most 7 nodes belonging to them.

We set the computing power, CP, to 1 in order to maximize malevolent abilities of the adversaries, also to show this trust model's greatest amount of resistance against the attacks.

We decided that in the case where the sum of direct trust and indirect trust was greater than 1, that only direct trust was used, resulting in following trust weight factors to be calculated as,

$$\alpha = \begin{cases} 1 & : DT + IndT > 1 \\ \frac{DT}{DT+IndT} & : 0 < DT + IndT \leq 1 \\ 0 & : DT + IndT = 0 \end{cases} \tag{2}$$

and,

$$\beta = 1 - \alpha \tag{3}$$

where the trust of node j calculated by node i under context c is,

$$T^c_{i,j} = \alpha \cdot DT_{i,j} + \beta \cdot IndT^c_{i,j}, \tag{4}$$

such that DT is the aggregation of direct trusts for all contexts, and $IndT$ is the aggregation of indirect trusts under context c for recommendations from each other node.

The effects of this can be seen Figure 1, where after approximately 20 transactions, the trust jumps from using a combination of direct and indirect to only using direct.

Nodes in this simulation were implemented to act benevolent with any context value less than or equal to the their randomly assigned context potential, under contexts above that they will act malevolent. A context, c_i is less than or equal to another context, c_j, iff $i \leq j$. The context setting adversaries attack by always reporting to the other nodes with a bad mouthed recommendation with the target context.

Parameter	Value
w	$\{0.25, 0.25, 0.25, 0.25\}$
w_h	0.50
w_d	0.50
R	0.5
CP	1
fb_{max}	10
MD	0.1
Contexts	$\{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}\}$
Total nodes	100
Transactions	50
Adversaries	30%

Table 1: The parameters of CBSTM IoT trust model implementation

2 Results

This trust model was resistant to the context attacks, due to the split of direct and indirect trusts, where direct trust is calculated as an aggregation of experiences in all contexts. Another factor that allowed for the mitigation of context attacks was the filtration of recommendations based on context, where the contexts themselves do not have any other effect on resulting trust calculation. Since the contexts were only used for the filtration of recommendations, standard bad mouthing mitigation techniques were effective against the context setting attack. The comparison of the context setting attack to a completely benevolent network is shown in Figure 1, where the red line is the trust values where 30% of network are context setting adversaries, and the blue line is when there are no adversaries in the network.

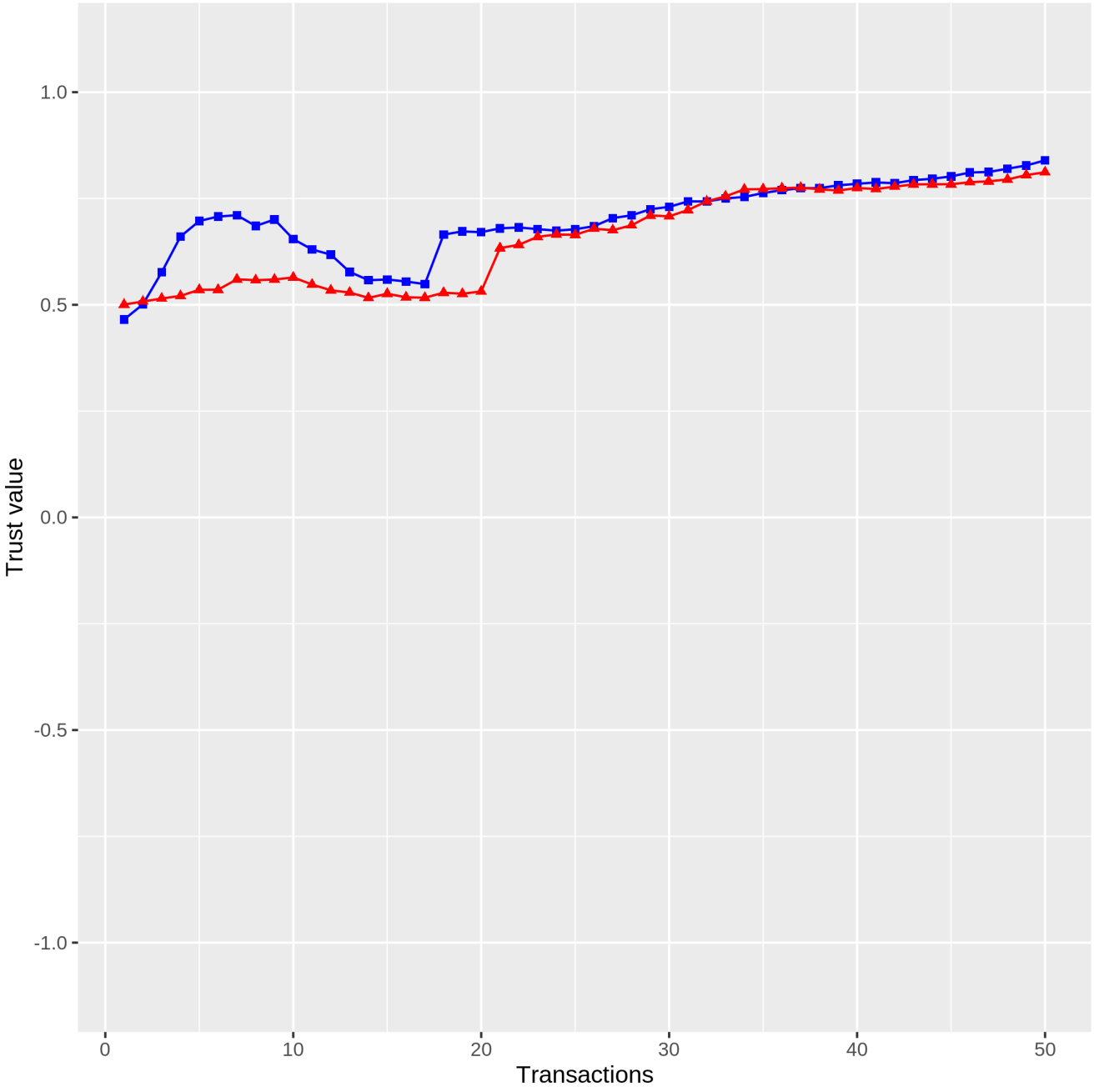

Figure 1: Comparison of the context setting attack to a benevolent network

References

[1] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In *Concurrency: the Works of Leslie Lamport*, pages 203–226. 2019.

[2] Sherif Emad Abdel Rafey, Ayman Abdel-Hamid, and Mohamad Abou El-Nasr. Cbstm-iot: Context-based social trust model for the internet of things. In *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, pages 1–8. IEEE, 2016.