A Social-based Watchdog Scheme to Detect Selfish Nodes in Mobile Social Networks

Behrouz Jedari
PhD candidate
email: bjedari@mail.dlut.edu.cn

Mobile and Social Computing Laboratory

Dalian University of Technology

28 September 2016

Outline

1. Introduction
2. Motivation and research questions
3. Proposed scheme
4. Experimental Results
5. Conclusion

1. Introduction

Mobile Social Networks (MSNs) [1] are emerging types of delay-tolerant networks (DTNs).

In MSNs, the nodes' **social features** are exploited to improve the routing performance.

Motivation: the nodes' social features have long-term characteristics. Meanwhile, the nodes tend to interact with nodes with whom they have strong social relationships.

[1] N. Vastardis, K. Yang, "Mobile Social Networks: Architectures, Social Properties, and Key Research Challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1355–1371, 2013.

1. Introduction (con..)

Major issues about selfish behavior in MSNs:

1. the impact of selfish behavior on data forwarding (my first research issue [2])
2. Incentive schemes (my second research issue [3])
3. **Selfish node detection**

[2] F. Xia, B. Jedari, L. T. Yang, J. Ma, and R. Huang, “A Signaling Game for Uncertain Data Delivery in Selfish Mobile Social Networks,” IEEE Transactions on Computational Social Systems, 2016.
[3] B. Jedari, L. Liu, T. Qiu, A. Rahim, F. Xia, "A Game-theoretic Incentive Scheme for Social-aware Routing in Selfish Mobile Social Networks," Future Generation Computer Systems, 2016.

1. Introduction (con..)

Detecting a selfish node in MSNs is challenging because:

- the network is fully distributed
- there is a lack of end-to-end connectivity between nodes

Watchdog systems: a promising detection mechanism in which some **trusted witness nodes** (called Watchdog nodes) analyze the routing behavior of their encountered nodes to detect their possible selfishness.

1. Introduction (con..)

Watchdog (W) nodes can acquire the watchdog information in two ways:

1. **Direct watchdog:** W nodes determine the selfish behavior of their encountered nodes based on the their forwarding messages
2. **Indirect watchdog:** W nodes share their (direct and indirect) watchdog information with each other

2. Motivation and Research Questions

The majority of existing watchdog schemes explore the **nodes' contact history** to identify dropped messages that result in **long detection time** and **high communication overhead**.

Besides, they assume a **social-oblivious altruism model** where the nodes' social ties do not affect their selfishness.

While our everyday experience shows that **rational selfish users** usually alleviate their selfishness level based on the strength of their social ties.

2. Motivation and Research Questions (con..)

The impact of selfishness in MSN routing can be more harmful when **malicious nodes** deliberately drop all incoming messages or a fraction of them but produce forged metrics about their forwarding behavior.

Consequently, the **main goal** is to detect selfish and misbehaving nodes **swiftly** and **accurately** with **minimum communication cost**.

2. Motivation and Research Questions (con..)

Thus, the following questions are raised:

1. How the nodes' social ties and content knowledge can be exploited to detect selfish nodes accurately with low communication overhead?
2. How the individual and social utility of messages forwarded by selfish nodes can help identify IS and SS nodes and their selfishness degree?

3. Proposed Scheme

we propose SoWatch scheme in which W nodes **analyze messages based on the nodes' social tie information** to detect selfish nodes (direct watchdog).

Meanwhile, nodes **exchange their opinions** about other nodes with each other to improve the detection time and accuracy (indirect watchdog).

Finally, we design **a reputation system** in which W nodes update the reputation of other nodes based on their direct and indirect watchdog information.

3. Proposed Scheme (con..)

Network Model: we consider a mobile MSN with N mobile nodes where the nodes are classified into three types:

1. Watchdog (W)
2. Selfish (S)
3. and Malicious (M) nodes

where |N| = |W| + |S| + |M|.

We assume the number of W nodes is higher than the other nodes.

3. Proposed Scheme (con..)

Message and Buffer Model

- Each message includes some properties (metadata)
- The buffer size of nodes is limited.
- Two types of messages can exist in the buffer of nodes:

1. Local messages
2. Non-local messages

Messages are generated based on correlated interaction [4]

[4] S. Okasha, "Altruism, group selection and correlated interaction," British Journal for the Philosophy of Science, vol. 56, pp. 4, pp. 703–725, 2005.

3. Proposed Scheme (con..)

Node Selfishness Model (Altruism model)

We suppose that S nodes are "**rational**" and "**social-aware**". Accordingly, we define the overall utility of a particular message m_b to a selfish node S as:

$$U_S(m_b, \alpha_S) = (1 - \alpha_S)U_S^{Ind}(m_b) + \alpha_S U_S^{Soc}(m_b)$$

$\alpha_S \in [0,1]$ is the social-awareness degree

3. Proposed Scheme (con..)

$$U_S(m_b, \alpha_S) = (1 - \alpha_S)U_S^{Ind}(m_b) + \alpha_S U_S^{Soc}(m_b)$$

In the equation above, we consider three conditions:

1. $\alpha_S = 0$: node S only cares about its own utility (i.e., S is an IS node).
2. $0 < \alpha_S \leq 0.5$: node S cares about the utility of her individual and social utilities (i.e., S is an SS node).
3. $0.5 < \alpha_S \leq 1$: node S cares about her social utility more than her individual utility that is not a rational behavior.

3. Proposed Scheme (con..)

Node Maliciousness Model

We consider three kinds of malicious behavior:

1. Message dropping
2. Manipulate contact records
3. Wrong information generation

3. Proposed Scheme (con..)

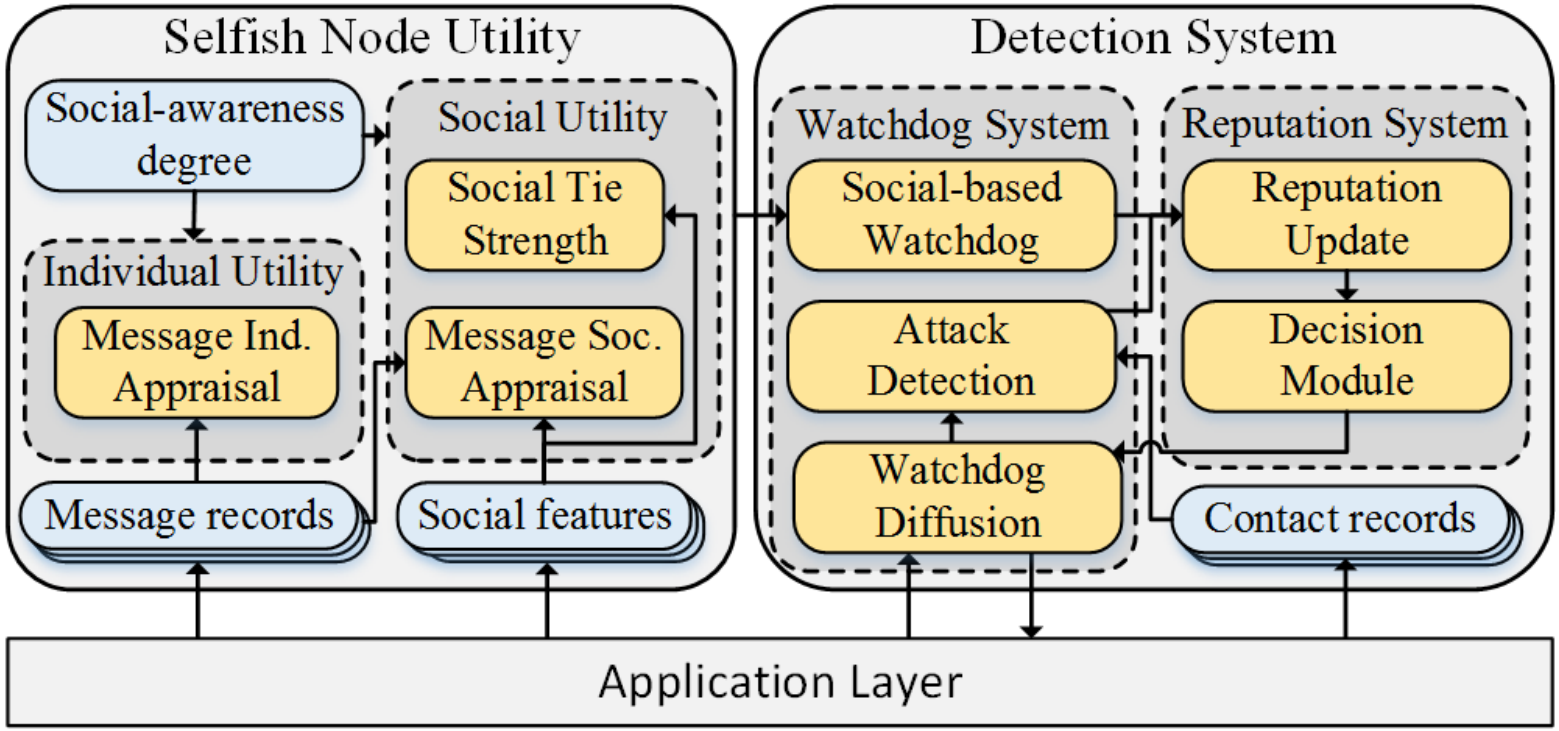


Figure 1: The architecture of the SoWatch scheme.

4. Performance evaluation

- We evaluate the performance of SoWatch using Opportunistic Network Environment (ONE) simulator [5].
- We use MIT Reality and Social Evolution [6] to set the Bluetooth contacts and social features of nodes.
- We compare the performance of SoWatch against a benchmark contact-based watchdog scheme [7].

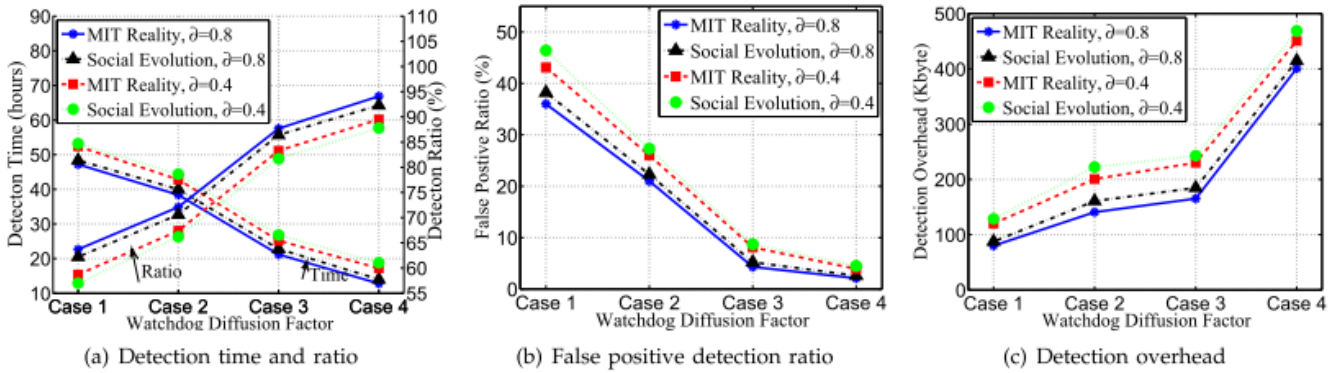
[5] A. Keranen, T. K¨arkkainen, and J. Ott, "Simulating mobility and DTNs with the one," Journal of Communications, vol. 5, no. 2, pp. 92–105, February 2010.
[6] MIT Human Dynamics Lab (hd.media.mit.edu)
[7] Q. Li and G. Cao, "Mitigating routing misbehavior in disruption tolerant networks," IEEE Trans actions on Information Forensics and Security, vol. 7, no. 2, pp. 664–675, 2012.

4. Performance evaluation (con..)

We evaluate four metrics in the simulations:

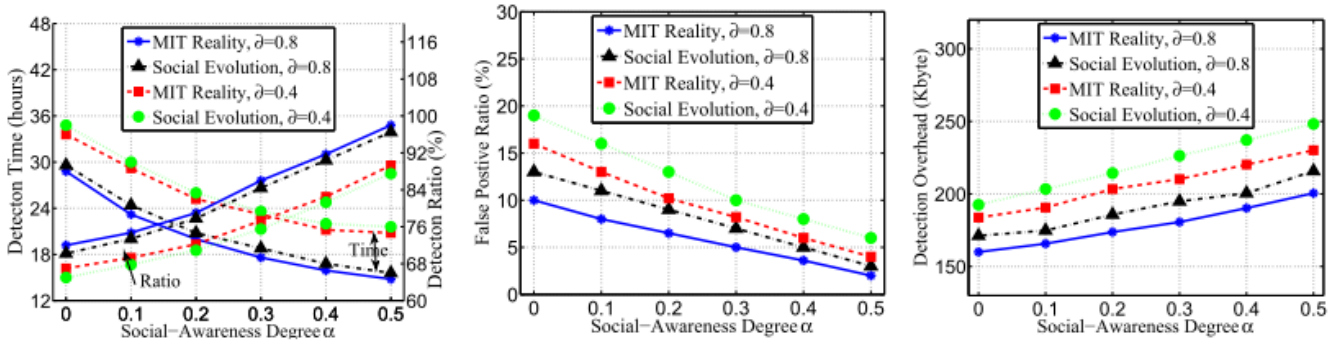
1. Selfish node detection time
2. Selfish node detection ratio
3. False positive detection ratio
4. Selfish node detection overhead

4. Performance evaluation (con..)



(a) Detection time and ratio (b) False positive detection ratio (c) Detection overhead

Fig. 3. The performance of the SoWatch scheme for different value of the watchdog diffusion factor over the MIT Reality and Social Evolution datasets when $\partial = 0.4$ and $\partial = 0.8$.



(a) Detection time and ratio (b) False positive detection ratio (c) Detection overhead

Fig. 4. The performance of the SoWatch scheme for different value of the social-awareness degree over the MIT Reality and Social Evolution datasets when $\partial = 0.4$ and $\partial = 0.8$.

4. Performance evaluation (con..)

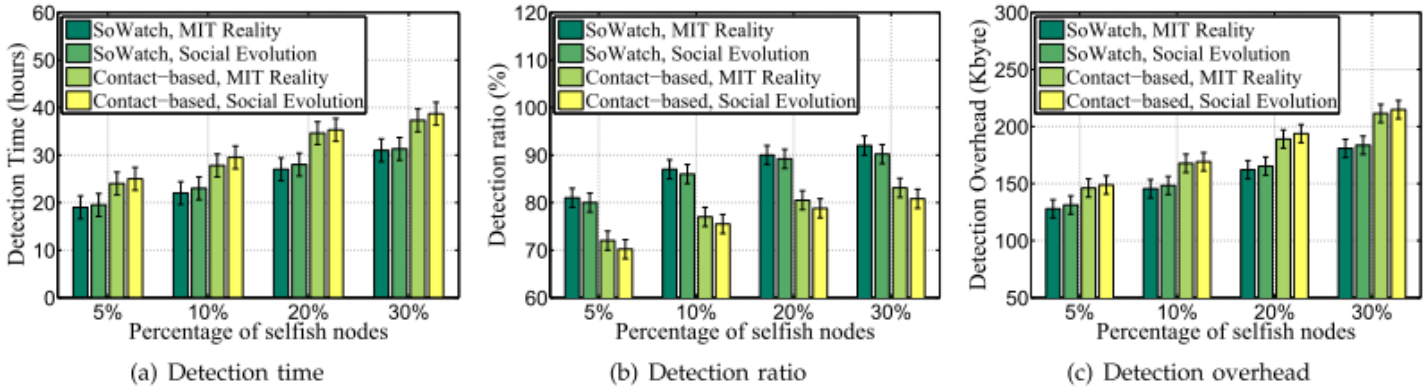


Fig. 5. The performance comparison of the algorithms with different ratio of selfish nodes over the MIT Reality and Social Evolution datasets. Standard deviations are shown using lines.

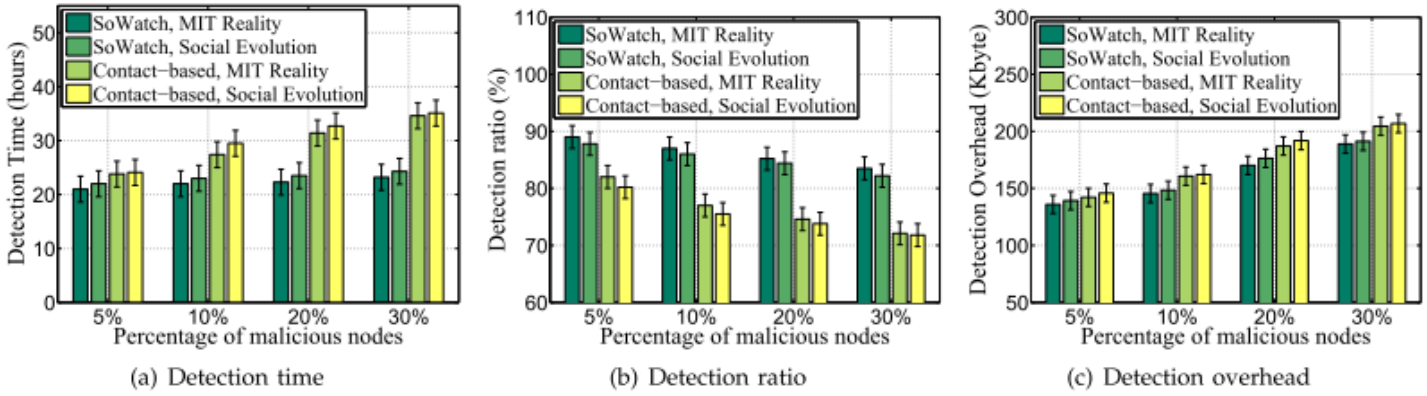


Fig. 6. The performance comparison of the algorithms with different ratio of malicious nodes.

5. Conclusion and Future Work

- We proposed a distributed social-based watchdog system (SoWatch) to detect selfish nodes in MSNs.
- The experimental results demonstrated that SoWatch outperforms a benchmark contact-based watchdog scheme in terms of the selfish node detection time, detection ratio, and communication cost.
- We plan to extend SoWatch to design an incentive scheme in energy-constrained socially selfish MSNs.

Thank you for your attention!