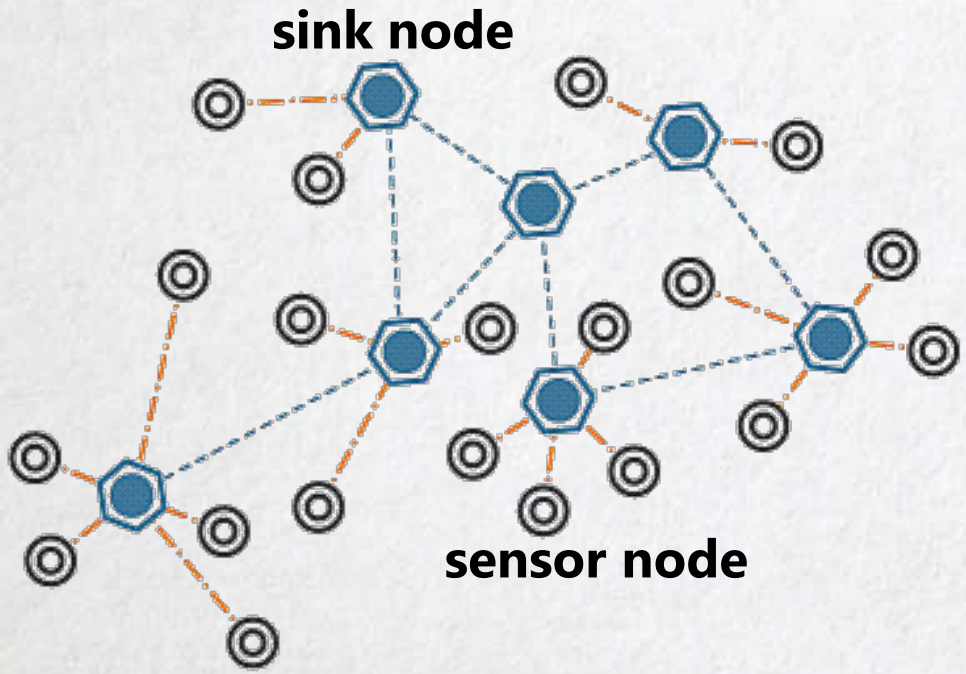
An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications

Junqi Duan, Deyun Gao, Dong Yang, Chuan Heng Foh and Hsiao-Hwa Chen
IEEE Internet of Things Journal, vol. 1, no. 1, pp. 58-69, Feb. 2014

Study Group Presentation

董皓文 2016.11.10

Wireless Sensor Networks, WSN



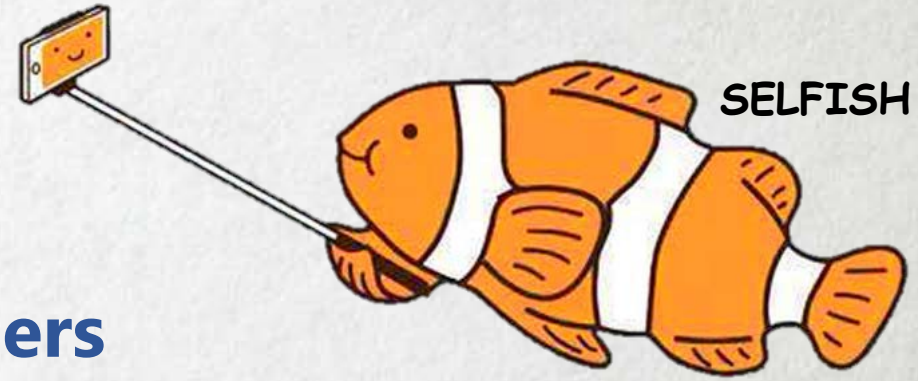
- Characteristics
  - **Power consumption constraints**
  - **Scalability**
  - Some mobility of nodes
  - Heterogeneity of nodes
  - Ability to withstand harsh environmental conditions
  - Ease of use
  - Cross-layer design

Background

- **Security issue**:
  - One of the **main challenges** for IoT
  - especially a **WSN-based IoT**
- WSN functions like medium access control (MAC) and routing protocols always **assume that the operating environment is trustworthy**.

Background – Cont'd

- However, WSNs are often deployed in **remote environments**
  - susceptible to attacks
  - difficult to protect physically



- Another Problem: **Selfish service providers**
  - Sensor nodes of different service providers may not completely cooperate with each other. For example, they may be configured for **resource conservation** which operate in a selfish manner.

Trust Evaluation

- In **public key infrastructure**
- Different definitions
- Usually composed of **direct trust** and **indirect trust**
  - **Direct trust**: direct observations of each node that participates in data communications
  - **Indirect trust**: obtained from recommendations of other nodes

Trust Evaluation - Procedure

- **Step 1 - trust derivation**
  - the process of collecting trust information
- **Step 2 - trust computation**
  - the process of calculating the synthesis trust value based on the observed direct trust and collected indirect trust
  - many have been proposed in recent years

Goals

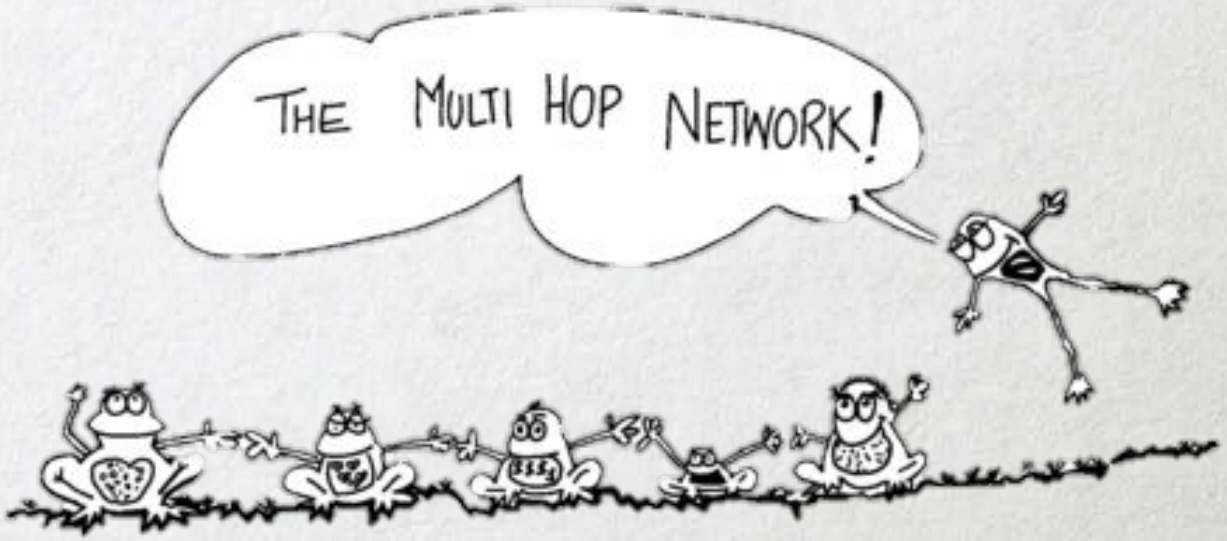
- A Proposal of an **energy-aware trust derivation scheme** for WSNs, which aims to
  - **minimize the energy consumption and latency of the network**
  - **under the premise of security assurance**.

Outlines

- **Risk Strategy Model**
  - derive the optimal number of recommendations.
- **Trust Derivation Dilemma Game, TDDG**
  - discuss the optimal ratio of gain to cost and the probability of the selected strategy based on the mixed strategy Nash equilibrium
- **Simulation Results and Performance Evaluation**
  - compare the energy consumption and latency of the network of the proposed schemes with traditional mechanisms

WSN Model

- a few sink nodes and a number of wireless sensor nodes.
- resource-constrained
- same limited radio coverage
- end-to-end communication via multihop relaying



Security Model

- **Assumptions: all sensor nodes are compromisable**
- while a sink node can be recognized as a highly trusted party in most cases with more sophisticated hardware

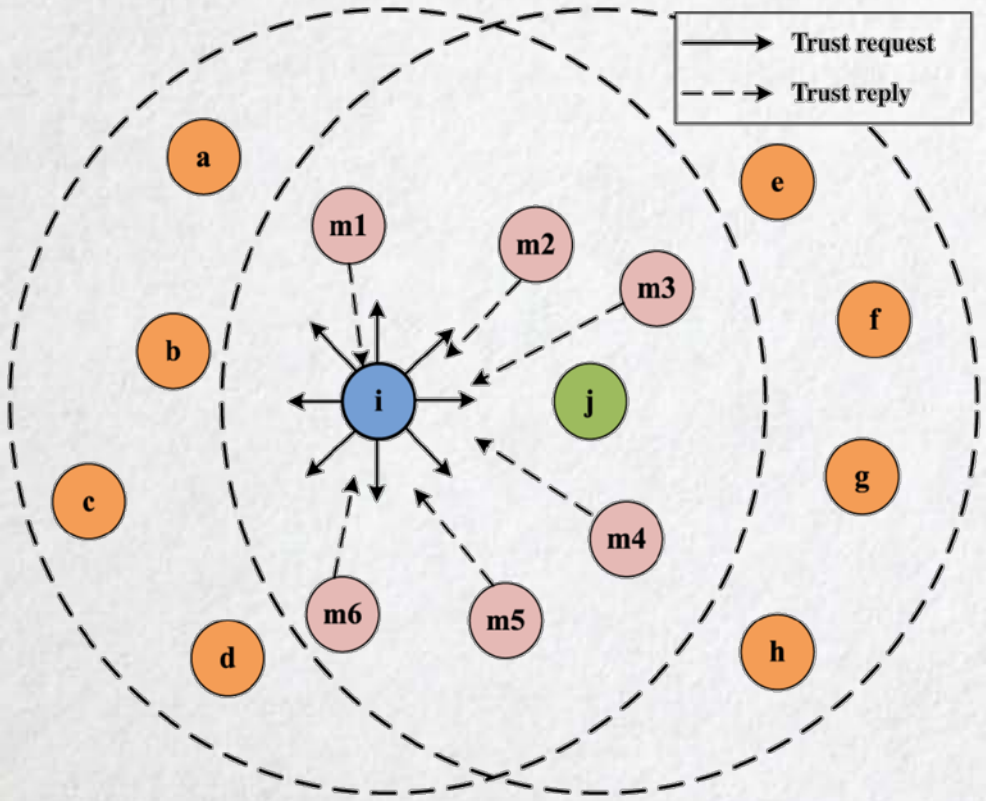
Security Model - Attacks

- **Passive attacks**
  - malicious nodes may **passively gather sensitive information** or **behave selfishly** in collaborative operations, such as routing
- **Active attacks**
  - malicious nodes may **actively request for sensitive information, influence the behavior of surrounding nodes or directly affect the normal operation of WSNs using attacks** such as denial of service (DoS)

Trust Model

- performs trust **derivation**, **computation**, and **application**
- detection mechanisms:
  - based on **watchdog**
  - each sensor node is responsible for monitoring the behavior of its neighbors within its radio range
- focus on **trust derivation**

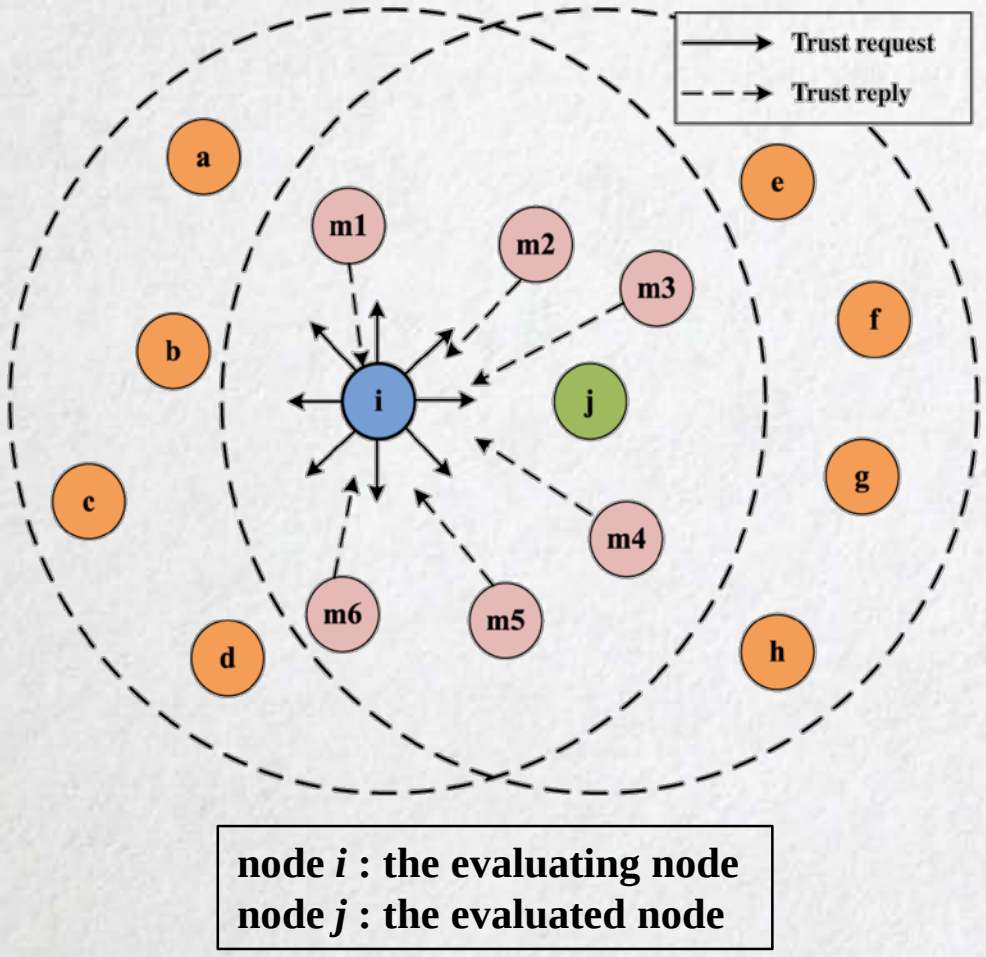
Network Risk Condition



- Let V be the set collecting all nodes in the network
- the minimum condition for the entire network to function properly:

$$R_j - \gamma f_g(e_j) \geq R_{th}, j \in V$$

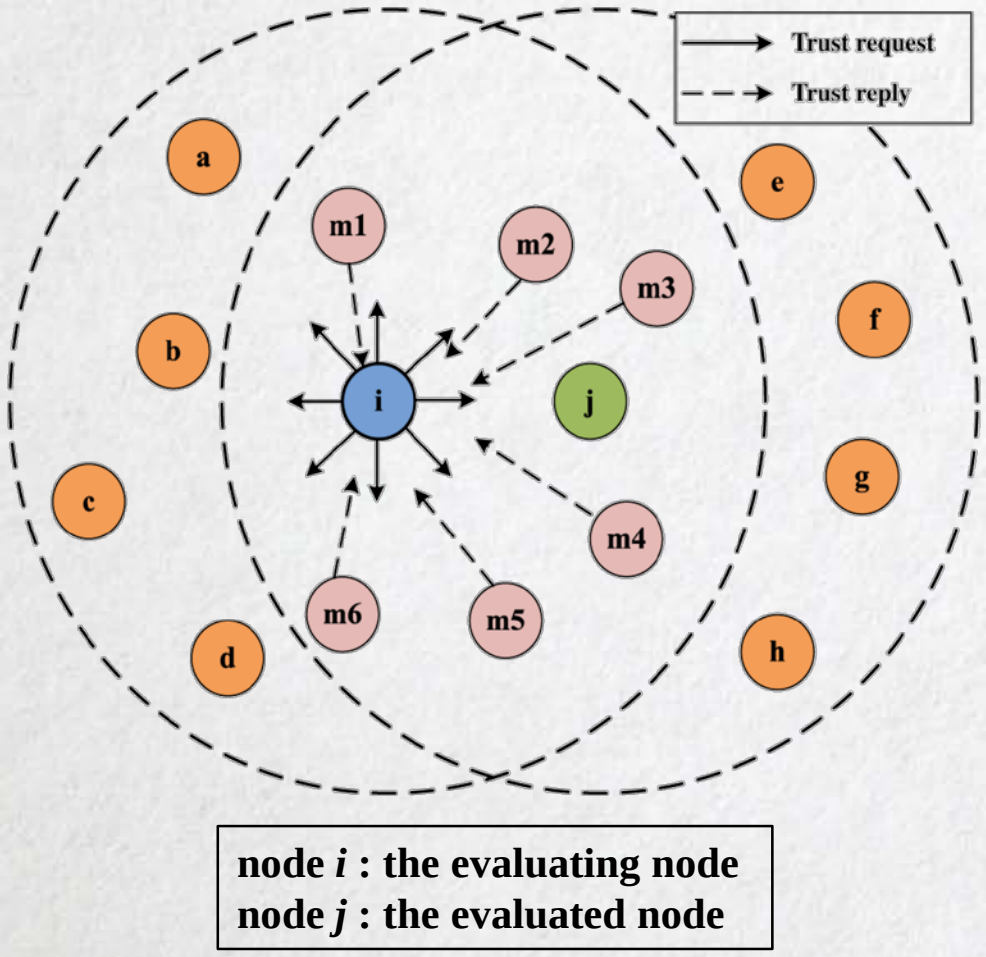
Network Risk Condition – Cont'd



$$R_j - \gamma f_g(e_j) \geq R_{th}, j \in V$$

- R_j: the reputation of node
- $f_g(e_j)$: energy saving for node j if it does not comply with a collection of proper behaviors e_j.
- γ: parameter specifying the ratio of reputation loss to energy saving

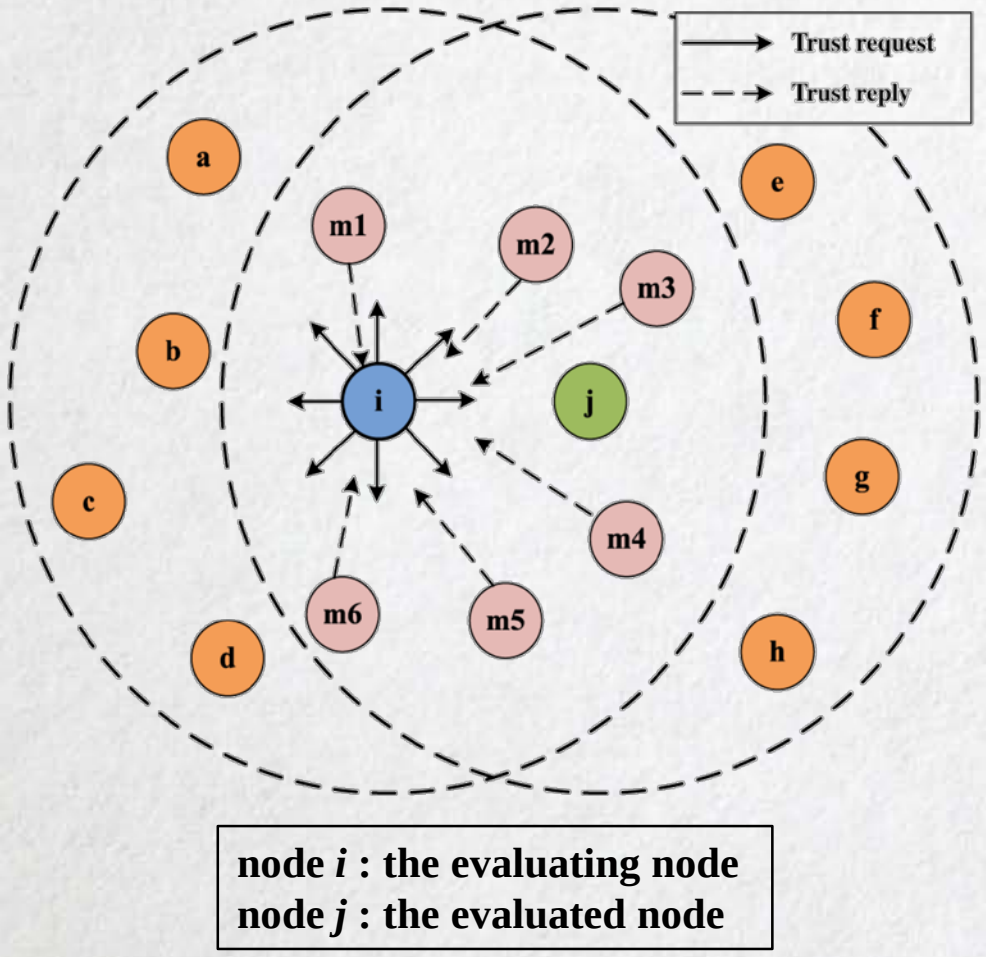
Network Risk Condition – Cont'd(2)



$$R_j - \gamma f_g(e_j) \geq R_{th}, j \in V$$

- R_{th}: a tolerable threshold such that the proper network function involving node *j* can be maintained if the overall reputation remains above R_{th}
- R_j and R_{th} are normalized to give values between 0 and 1

Network Risk Condition – Cont'd(3)



$$R_j - \gamma f_g(e_j) \geq R_{th}, j \in V$$

- From the node's prospective, **if it attempts any improper behavior, it will be penalized by lowered reputation rating**

Instantaneous Reputation

- risk and reputation are evaluated **periodically**
- the **instantaneous reputation** of node *j*
  - also the **overall trust value at round *l***
  - defined as **the difference between the positive and negative trust assessments** combined from direct and indirect observations

$$R_j = \Delta T_j^{(l)} = f_t\left(\Delta T_D(i,j)^{(l)}, \Delta T_I\left(M_j, j\right)^{(l)}\right)$$

Instantaneous Reputation – Cont'd

- the **instantaneous reputation** of node *j*

$$R_j = \Delta T_j^{(l)} = f_t\left(\Delta T_D(i,j)^{(l)}, \Delta T_I\left(M_j, j\right)^{(l)}\right)$$

  - $\Delta T_D(i,j)^{(l)}$: **overall direct trust value** of node j for node *i* at *l*-th round
  - $\Delta T_I\left(M_j, j\right)^{(l)}$: **overall indirect trust value** of node *j* for node *i* at *l*-th round
  - M_j: the set of nodes **providing recommendations** of node *j* for node *i*
  - $f_t(\cdot)$: function that defines **how direct and indirect trust values are consolidated**

Instantaneous Reputation Computation

- Let A be the set containing **all defined network activities**
  - $\boldsymbol{P_j(a)}$: Positive or well-behaved activities
  - $\boldsymbol{N_j(a)}$: negative or misbehaved activities
- the importance of each predefined activity is **predetermined** and specified as **weight functions** in $\boldsymbol{P_W(a)}$ and $\boldsymbol{N_W(a)}$

$$\sum_{a \in A} \boldsymbol{P_W(a)} = \sum_{a \in A} \boldsymbol{N_W(a)} = \mathbf{1}$$

Overall Direct Trust Value

previous direct trust value

weight

$$\Delta T_D(i,j)^{(l)} = \sum_{a \in A} f_d\left(T_D(i,j)^{(l-1)}, P_j(a)^{(l)}\right) P_W(a)$$

current assessment of a behavior

$$- \sum_{a \in A} f_d\left(T_D(i,j)^{(l-1)}, N_j(a)^{(l)}\right) N_W(a)$$

- $f_d(\cdot)$ defines the combination of the **previous trust value** and the **current assessment of a behavior**

Overall Indirect Trust Value

previous indirect trust values

current assessment of a behavior

$$\Delta T_I(M_j, j)^{(l)} = \sum_{a \in A} f_r\left(T_I(m_1, j)^{(l-1)}, T_I(m_2, j)^{(l-1)}, \dots, T_I(m_n, j)^{(l-1)}, P_j(a)^{(l)}\right) P_W(a) - \sum_{a \in A} f_r\left(T_I(m_1, j)^{(l-1)}, T_I(m_2, j)^{(l-1)}, \dots, T_I(m_n, j)^{(l-1)}, N_j(a)^{(l)}\right) N_W(a)$$

- where $m_1, m_2, \dots, m_n \in M_j$
- $f_r(\cdot)$ defines the combination of the **previous trust value** and the **current assessment of a behavior**

Energy Saving Function

- Without loss of generality, we set **energy cost to be directly proportional to the overall trust value ΔT_j.**
  - i.e. the energy saving of an improper behavior is linear to the reduction in the trust value.

$$\frac{\Delta T_j}{T_{max}} = \frac{\Delta E_j}{E_{max}}$$

- $T_{max} = 1$ by definition of reputation

$$\Delta E_j = \Delta T_j \cdot E_{max}$$

Network Risk Condition

$$R_j - \gamma f_g(e_j) \geq R_{th}, j \in V$$

$$f_t\left(\Delta T_D(i,j), \Delta T_I(M_j,j)\right) \geq R_{th} + \gamma \Delta T_j E_{max}, j \in V$$

- the specifications of $f_t(\cdot)$ is shown in the previous works
- performance closely associate with **the number of recommendations**

Number of Recommendations

- In indirect trust value
  - computed by **the combination of all received recommendations**
  - acquiring **adequate number of recommendations** is important to make reliable judgement on trustworthiness of a node
- Ideally, we hope to collect **all** recommendations.
  - BUT **communication overheads** results in high energy consumption

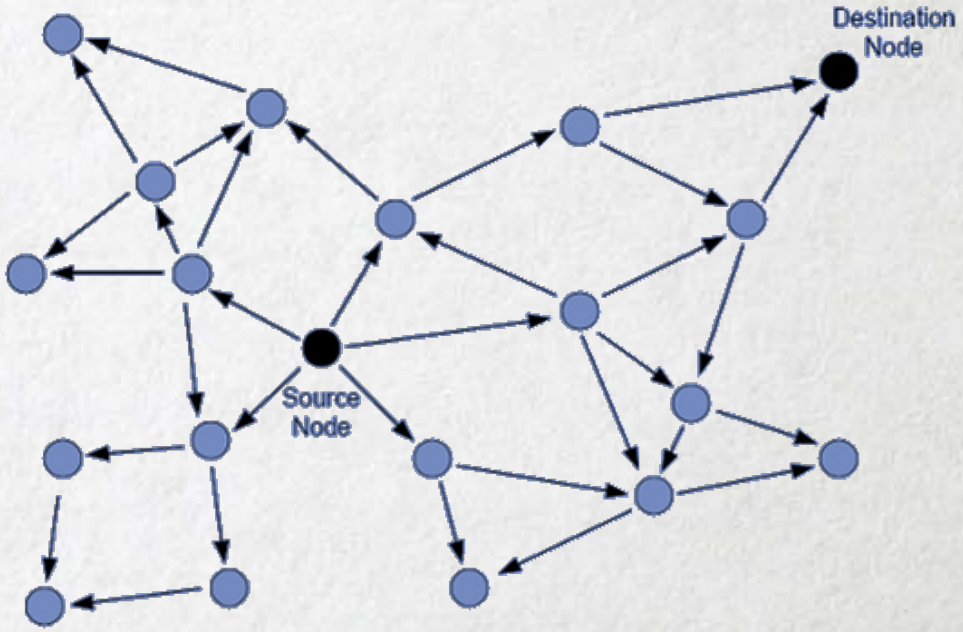
Optimal Number of Recommendations

$$k = min\left\{\left\|\Omega\left(\Delta T_I(M_j, j)\right)\right\|\right\}$$

- $\Omega(\cdot)$: all possible combinations of neighbor selections for recommendations that satisfy the network risk condition, i.e. $R_j - \gamma f_g(e_j) \geq R_{th}, j \in V$

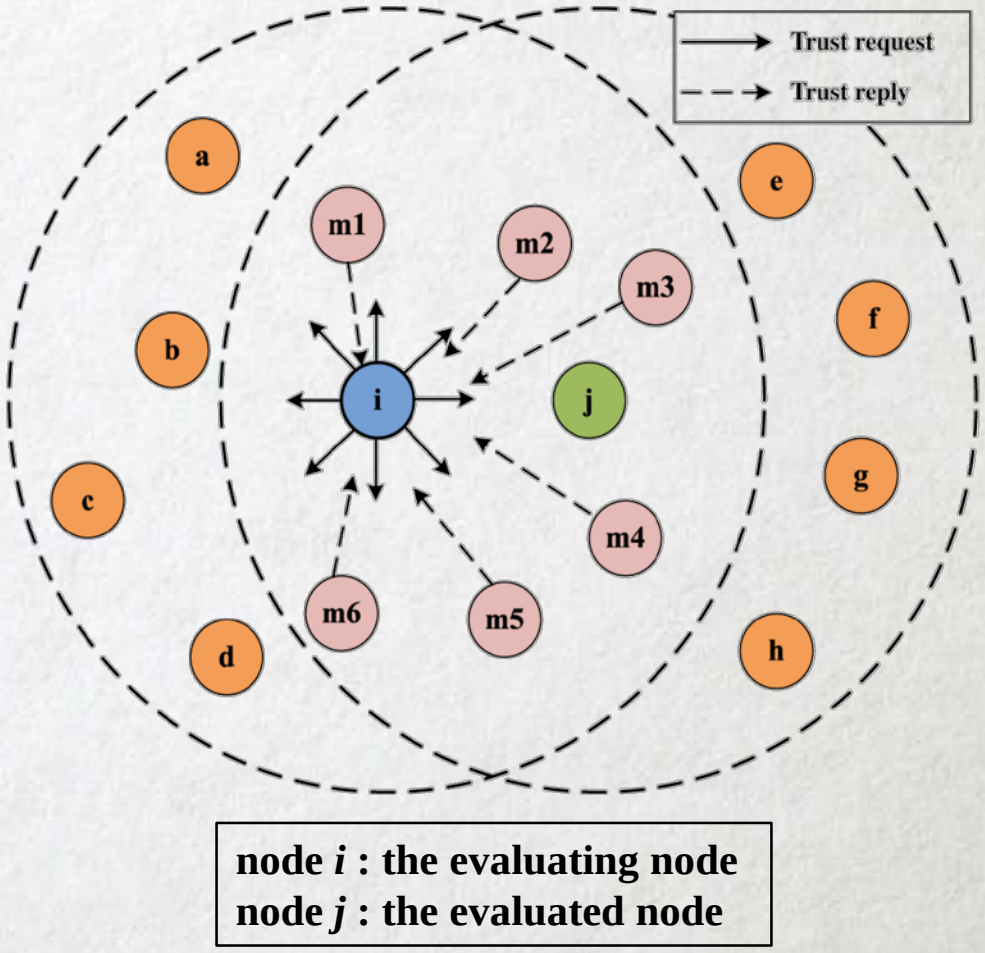
Trust Derivation Procedure

- **flooding**
  - often been adopted
  - broadcast trust information to **all** other nodes in the network.
  - ensure adequate collection of trust information for all users
  - BUT **energy consumption**
  - BUT **lengthy latency**



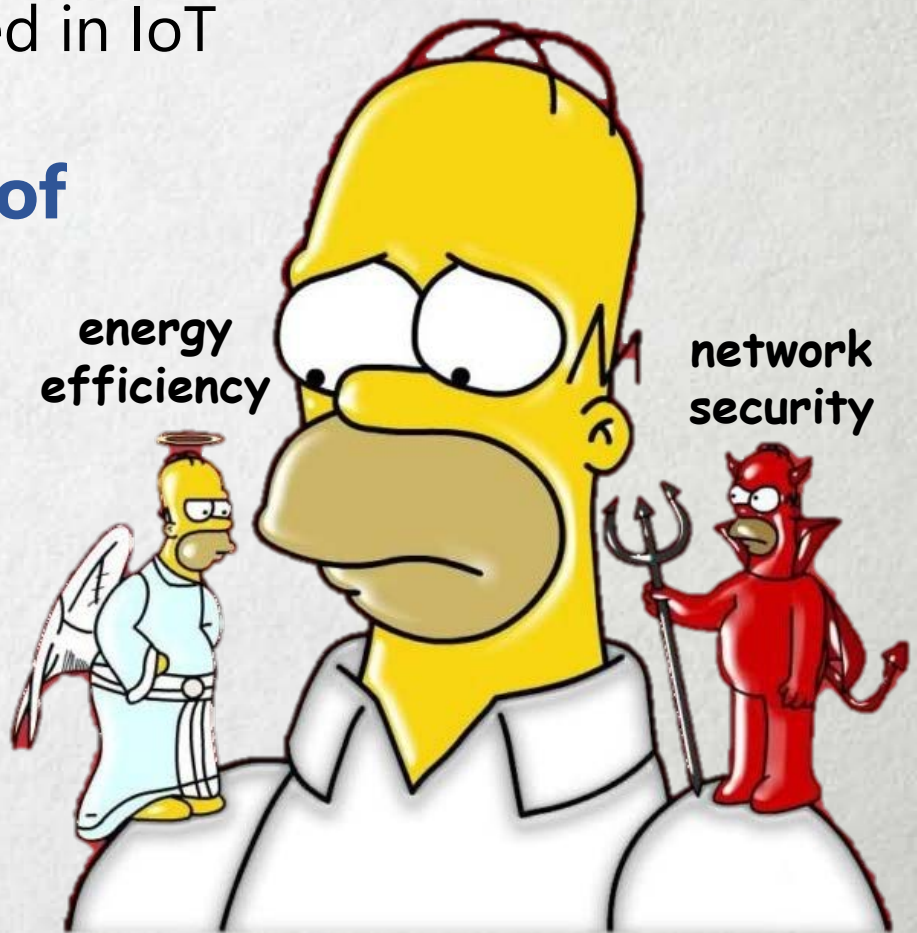
Trust Derivation Procedure – Cont'd

- **hop limit value**
- ONLY recommendations from **the neighbor nodes of the evaluated node** are chosen



Trust Derivation Procedure – Cont'd

- **Problem**: the effect may be limited
  - especially in a **dense network** often considered in IoT
- **Solution:** receiving nodes **make decision of whether to send a trust reply**
  - a **dilemma** game, TDDG
  - **energy efficiency** vs **network security**
  - a smaller number: security challenges
    a higher number: unnecessary overheads

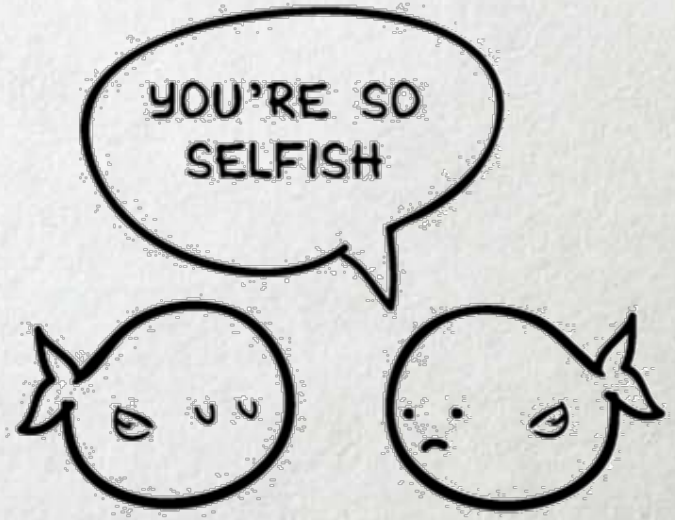


Trust Derivation Dilemma Game(TDDG)

- Recall:

$$k = min\left\{\left\|\Omega\left(\Delta T_I(M_j, j)\right)\right\|\right\}$$

  - only in ideal environment where **all nodes behave cooperatively**
  - **potential selfishness** in the process
    - **game theoretic approach**



TDDG – Game Model

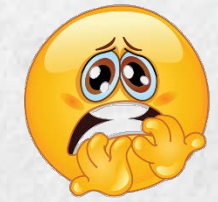
- Players: N **nodes**
  - N is the number of the specified evaluated node's neighbors except the evaluating node
- Strategies: **Reply** or **Not Reply**
  - Reply: reply to the evaluating node when receiving trust request
  - Not Reply: disregard the trust request when receiving it.
- The network is **secure** if and only if

$$\#(\textbf{recommendations}) \geq k$$

TDDG – Game Model – Cont'd

- **When $N \leq k$**
  - the network may not be secure even all the neighbors of the evaluated node reply the trust request
  - **all the neighbors must reply** to reduce the security risk
- **When $N \geq k$**
  - every participating node makes a decision: **whether to reply the trust request or not**

participating node



TDDG – Game Model – Utility

- **Utility function**
  - G: the utility when #($participating\ nodes\ that\ choose\ to\ reply$) $\geq k$
- **Cost function**
  - Assumption: the cost is **the same** for every node
  - $f_s(e)$: cost to send trust reply
- **Assumption**
  - **the gain from security exceeds the optimal cost to send trust reply**

$$G > kf_s(e) > 0$$

TDDG, k=1

PAYOFF MATRIX FOR TDDG ($k = 1$)

TDDG ($k = 1$)		Other nodes ($N - 1$)	
		No Other Reply	At Least One Reply ($1 \leq \alpha \leq N - 1$)
Node i	No Reply	$0, 0$	$G, G - \alpha f_s(e)$
	Reply	$G - f_s(e), G$	$G - f_s(e), G - \alpha f_s(e)$

- **Concept**: A node prefers to keep silence to save energy if it thinks that at least another node will send trust reply.
- **Probabilistic modeling**: for an arbitrary node
  - sends trust reply with probability $\boldsymbol{p}$
  - remains silence with probability $\boldsymbol{1 - p}$.

TDDG, k=1

PAYOFF MATRIX FOR TDDG ($k = 1$)

TDDG ($k = 1$)		Other nodes ($N - 1$)	
		No Other Reply	At Least One Reply ($1 \leq \alpha \leq N - 1$)
Node i	No Reply	$0, 0$	$G, G - \alpha f_s(e)$
	Reply	$G - f_s(e), G$	$G - f_s(e), G - \alpha f_s(e)$

- For N nodes, $\mathbf{P}$(at least one node reply) $= \mathbf{1} - (\mathbf{1} - \boldsymbol{p})^{\boldsymbol{N-1}}$
- **mixed strategy NE**

$$\boldsymbol{G\left(1 - (1 - p)^{N-1}\right) = G - f_s(e) \quad or \quad p = 1 - \left(\frac{f_s(e)}{G}\right)^{\frac{1}{N-1}}}$$

TDDG, $k>1$

PAYOFF MATRIX FOR TDDG ($k > 1$)

TDDG ($k > 1$)		Other nodes ($N-1$)		
		α Nodes Reply ($0 \leq \alpha < k-1$)	$k-1$ Nodes Reply	β Nodes Reply ($k-1 < \beta \leq N-1$)
Node i	No Reply	$0, -\alpha f_s(e)$	$0, -(k-1) f_s(e)$	$G, G - \beta f_s(e)$
	Reply	$-f_s(e), -\alpha f_s(e)$	$G - f_s(e), G - (k-1) f_s(e)$	$G - f_s(e), G - \beta f_s(e)$

- **Idea**: a node will prefer to reply the trust request if and only if it **believes that other $k-1$ nodes will send trust reply**. Otherwise, it prefers to keep silence to conserve energy.
- **P(k nodes choosing reply strategy)** $= C_N^k p^k (1-p)^{N-k}$

TDDG, $k>1$

- Solution to the **mixed strategy NE:**

$$C_{N-1}^{k-1} p^{k-1} (1-p)^{N-k} = \frac{f_s(e)}{G}$$

$$\frac{k-1}{N-1} \leq p < 1, G \geq C_{N-1}^{k-1} \left(\frac{k-1}{N-1}\right)^{k-1} \left(\frac{N-k}{N-1}\right)^{N-k}$$

TDDG

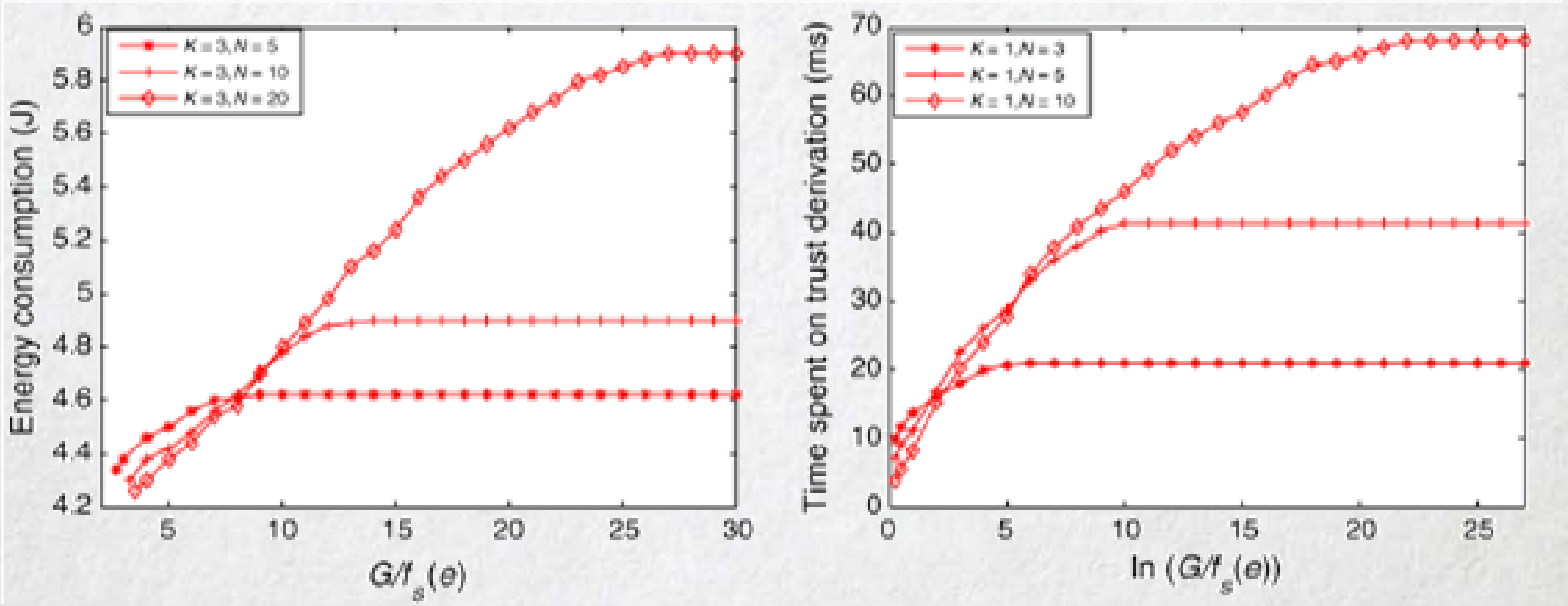
- For both case $k = 1$ and case $k > 1$,

  the probability $\boldsymbol{p}$ depends on the selection of $\boldsymbol{G/f_s(e)}$

Simulation Results – Selection of $G/f_s(e)$

- $G/f_s(e)$ should be **kept small** for **lower energy consumption** and **shorter latency**.

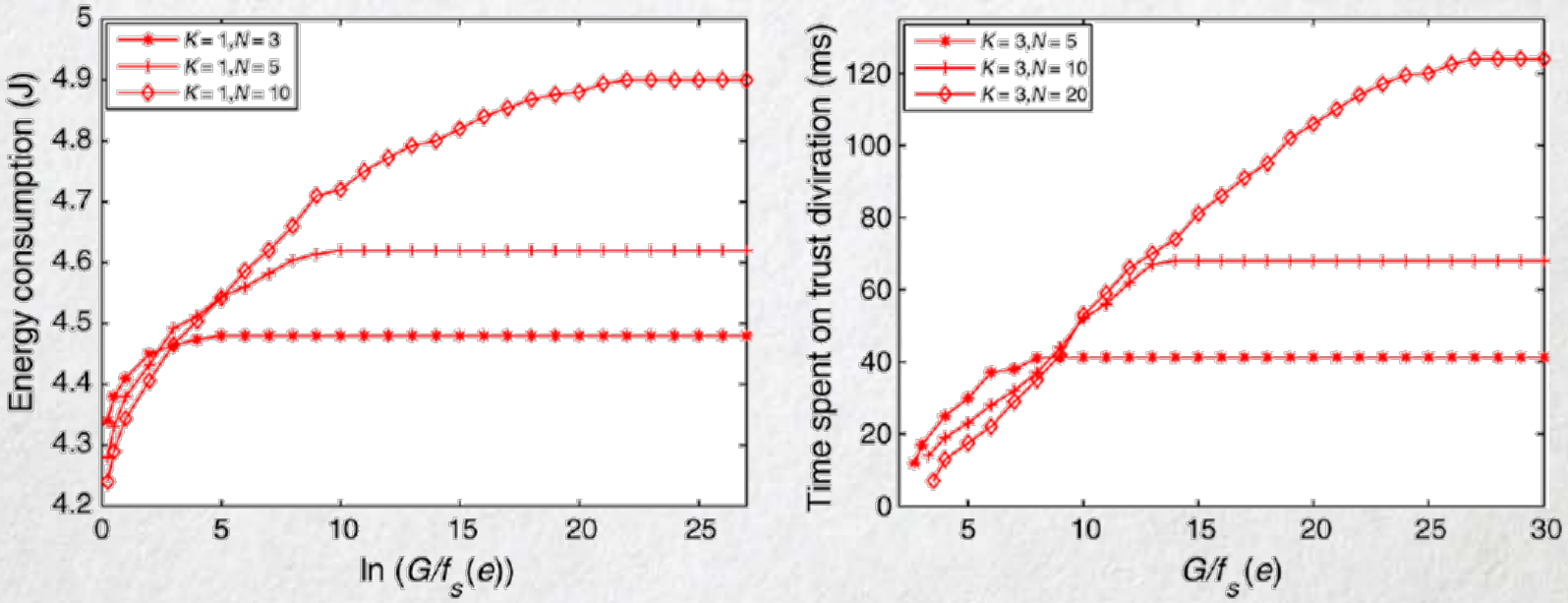
$$k = 1$$



Selection of $G/f_s(e)$ – Cont'd

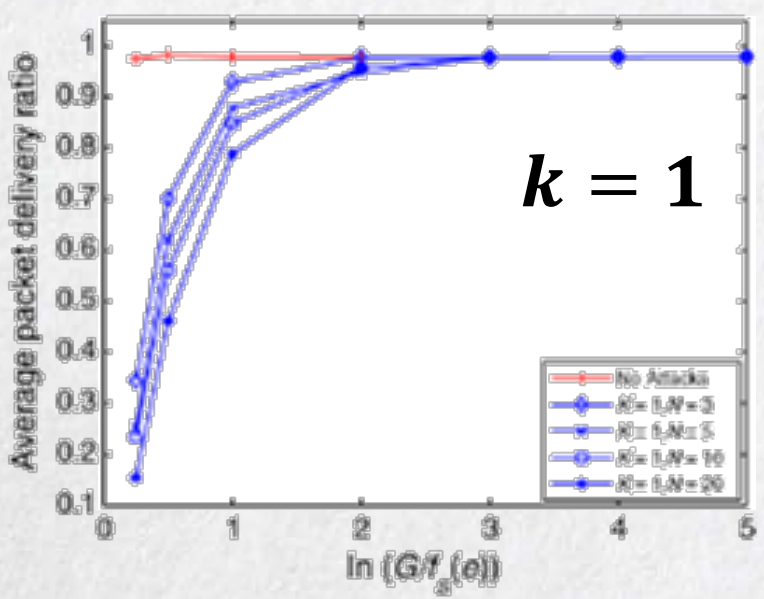
- $G/f_s(e)$ should be **kept small** for **lower energy consumption** and **shorter latency**.

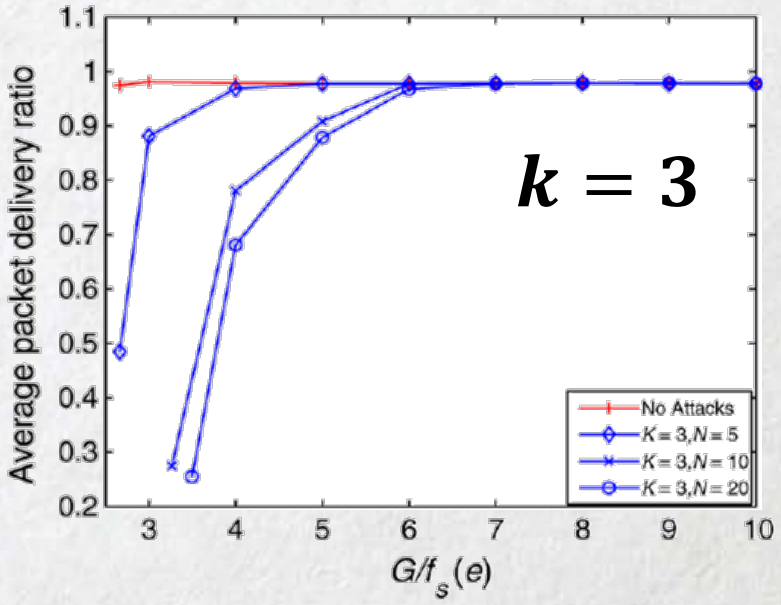
$$k = 3$$



Selection of $G/f_s(e)$ – Cont'd

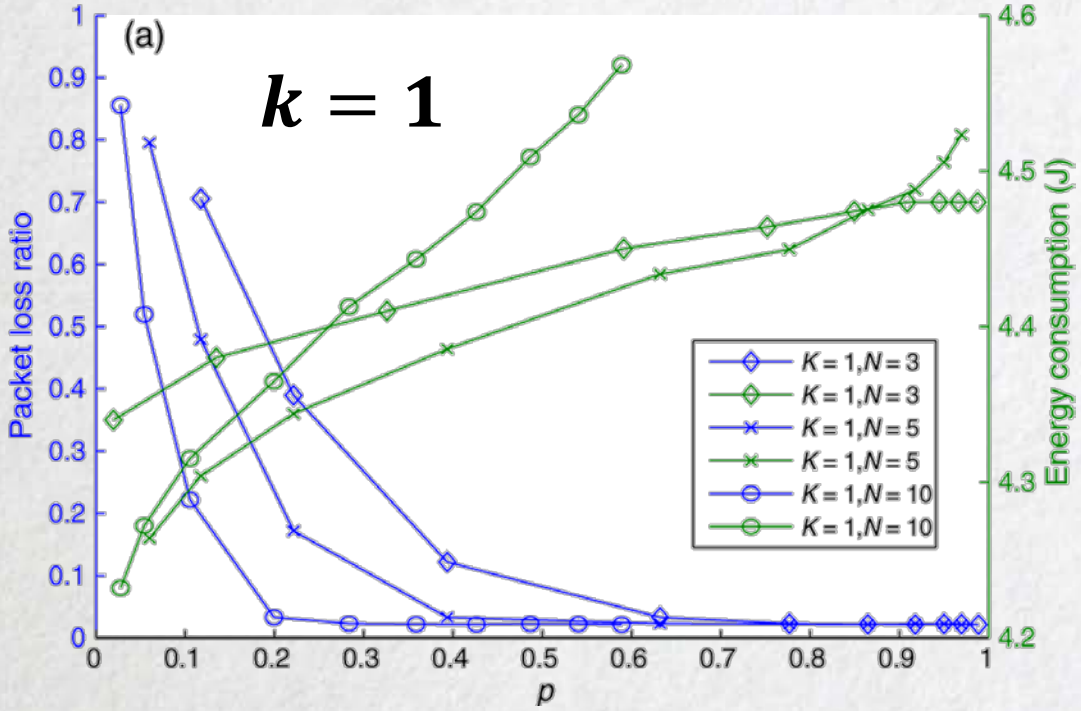
- **BUT** if $G/f_s(e)$ is **not adequately large**, selfish users may refuse to reply and thus fewer than intended replies will be returned which may **reduce the quality of the recommendation**.

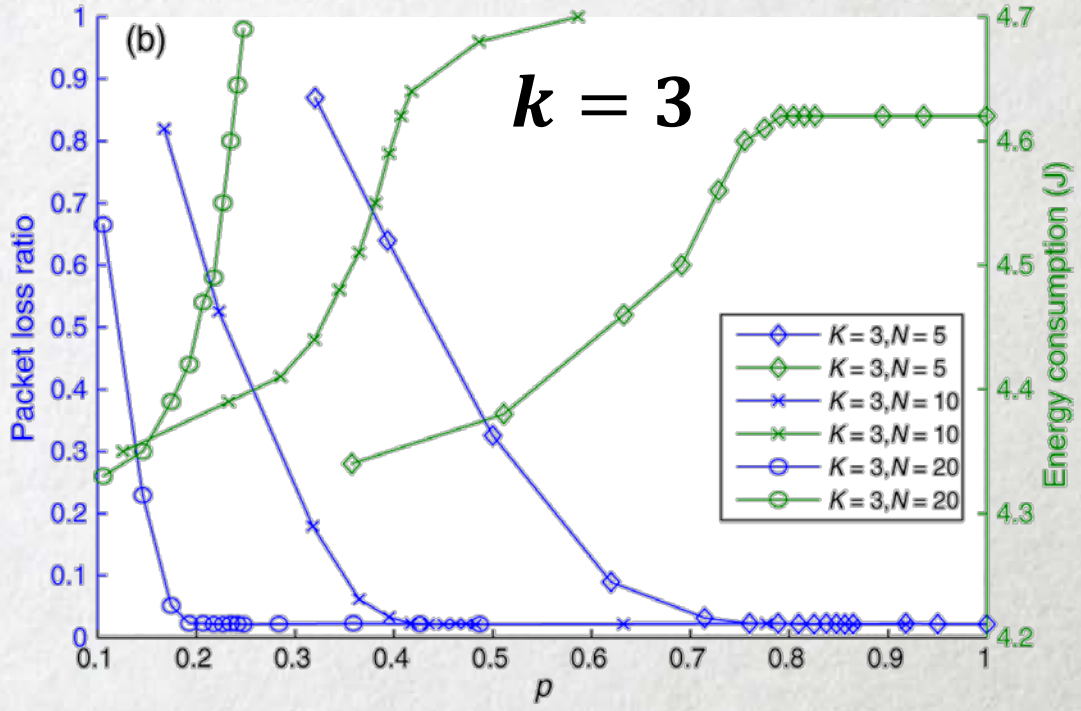




Selection of $G/f_s(e)$ – Cont'd

- the **tradeoff** between **energy efficiency** and **security**





Analysis of Attacks on Trust Derivation

- **Trust Management Systems**:
  - deal with most of the conventional attacks in WSNs
  - BUT some malicious nodes or misbehaved nodes(MNs) may possibly be **incorrectly included** in the trusted set of nodes that provide recommendations at some point

Common Attacks to a Trust Management System for WSNs

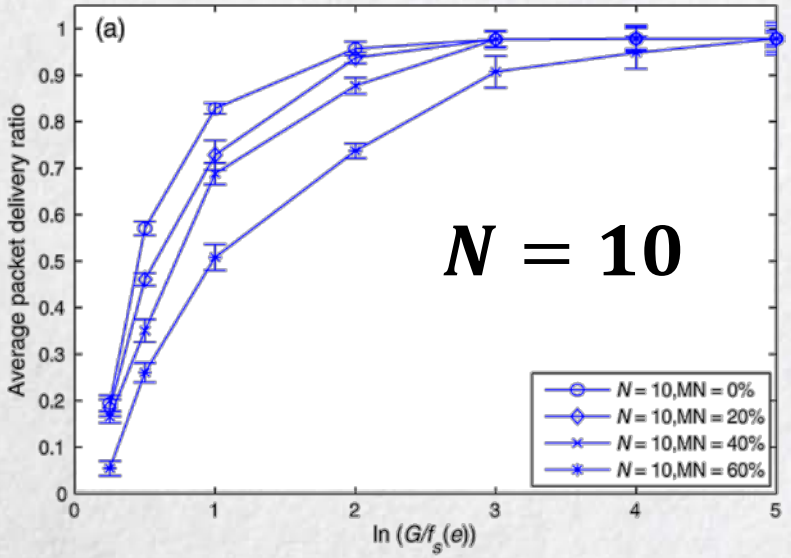
- **Bad mouthing attack**
  - The MNs provide false recommendations and propagate negative reputation information about well-behaved nodes
  - can be solved by **using an inconsistency check scheme** in trust derivation process to detect MNs and filter out false recommendations
- **DoS attack**
  - A DoS attacker can disrupt legitimate communication of other nodes by flooding the network with redundant recommendations.
  - can be solved by **limiting the data generation rate of the source node** or **adopting the DoS-resistant network architecture** such as NetFence

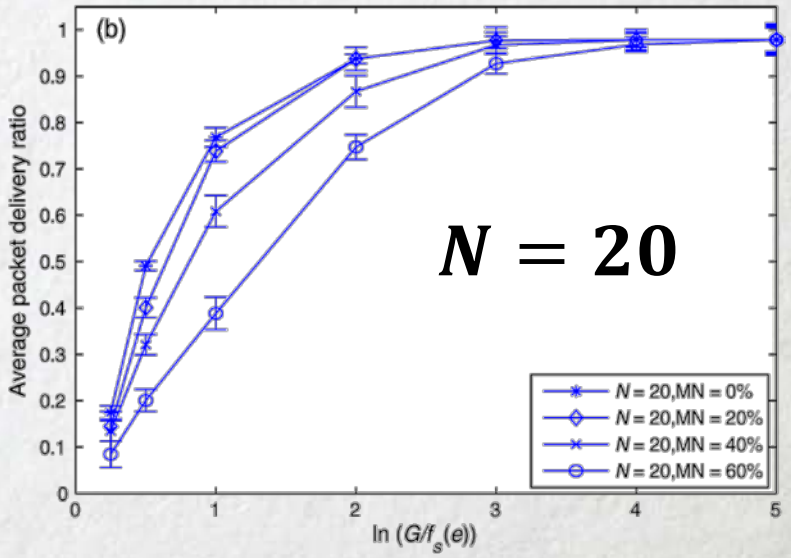
Common Attacks to a Trust Management System for WSNs

- **Selfish attack**
  - A selfish node may not follow the policies in TDDG. When receiving the trust request, it will simply drop the request and not send trust reply by preserving its resources.
  - can be solved by **increasing the value of** $G/f_s(e)$ to ensure the security of the network.

Simulation Results – Effect of MNs, k=1

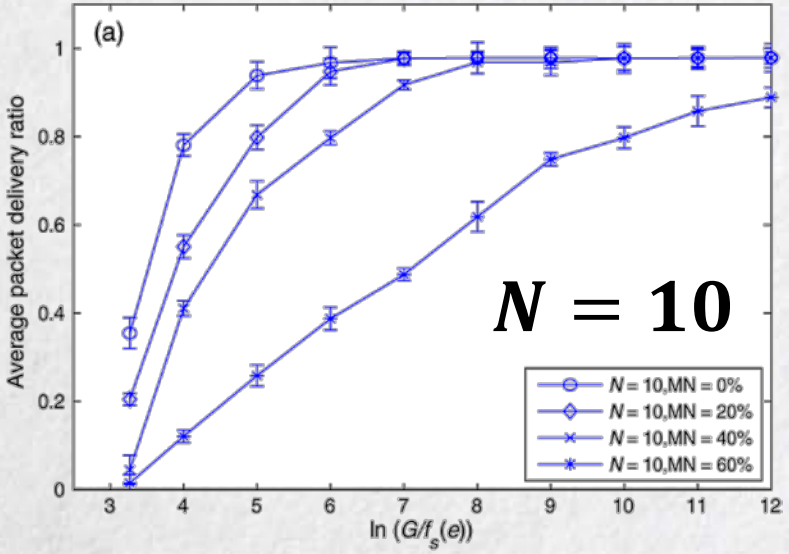
- The **minimum $G/f_s(e)$** that satisfies the network security condition **increases as the proportion of MNs rises**
  - Because the actual number of participating nodes is less than the theoretical value, as the MNs do not follow the policies in TDDG.

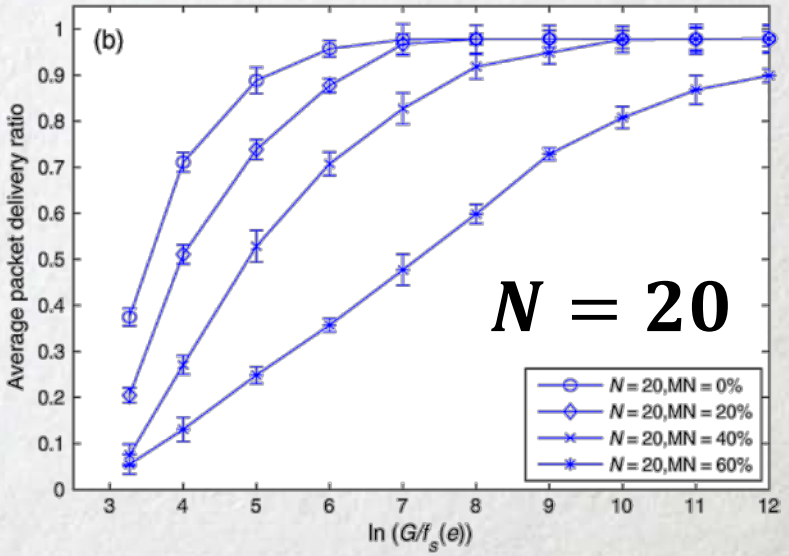




Simulation Results – Effect of MNs, k=3

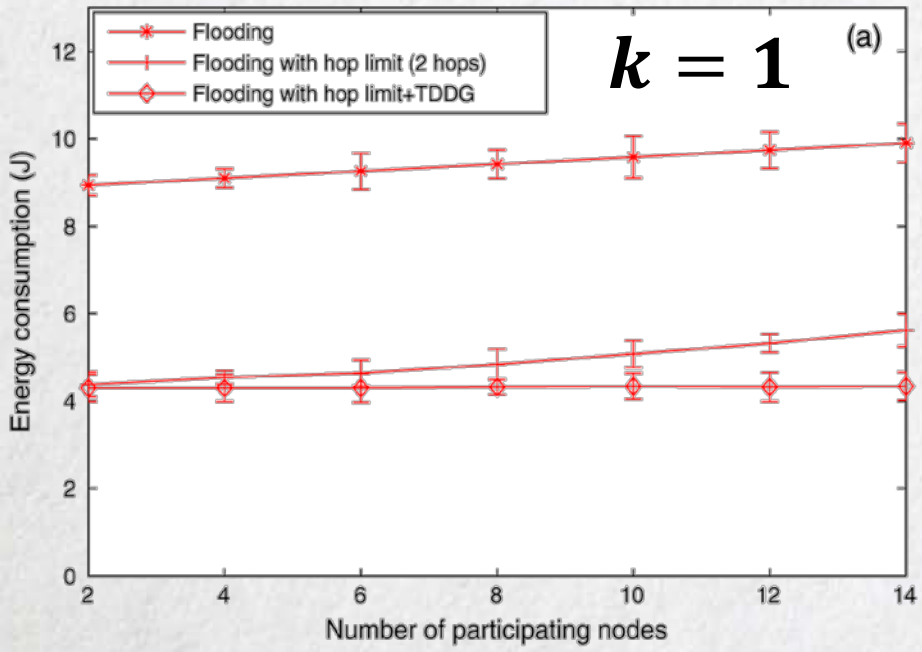
- The **minimum $G/f_s(e)$** that satisfies the network security condition **increases as the proportion of MNs rises**
  - Because the actual number of participating nodes is less than the theoretical value, as the MNs do not follow the policies in TDDG.

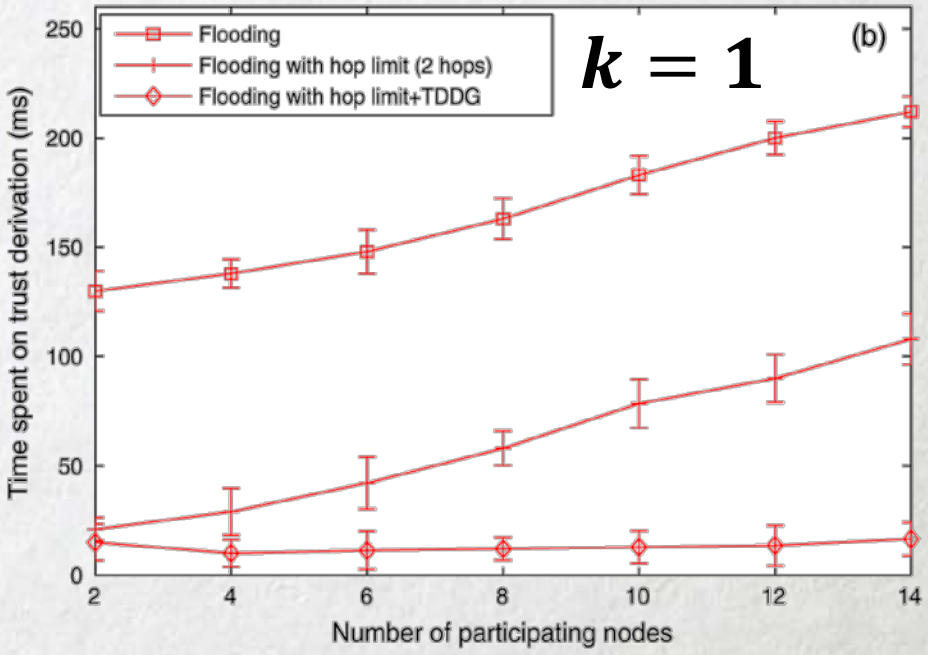




Simulation Results – Performance Evaluation

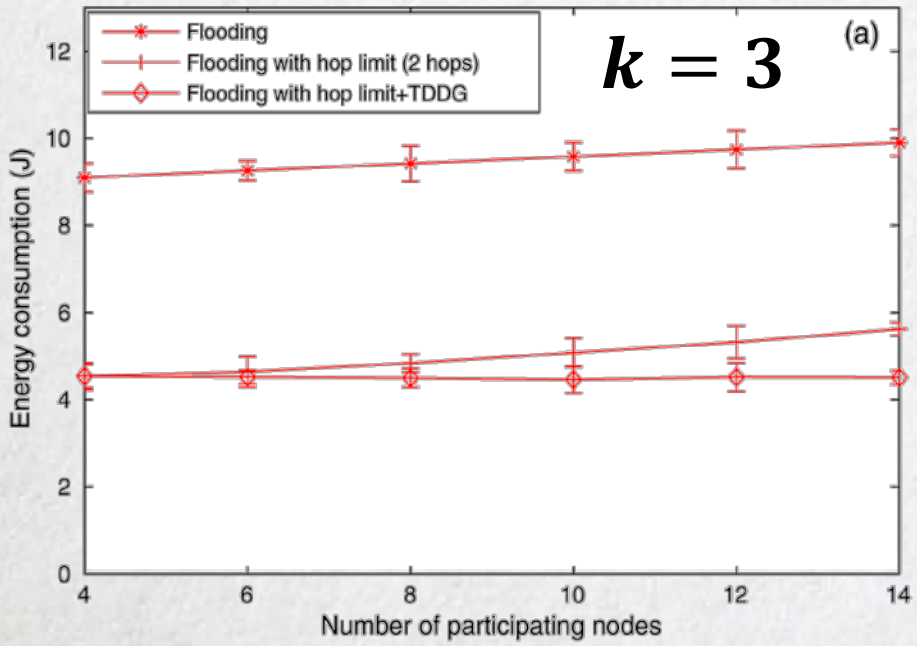
- The energy consumption of **flooding** is much higher than the other two schemes

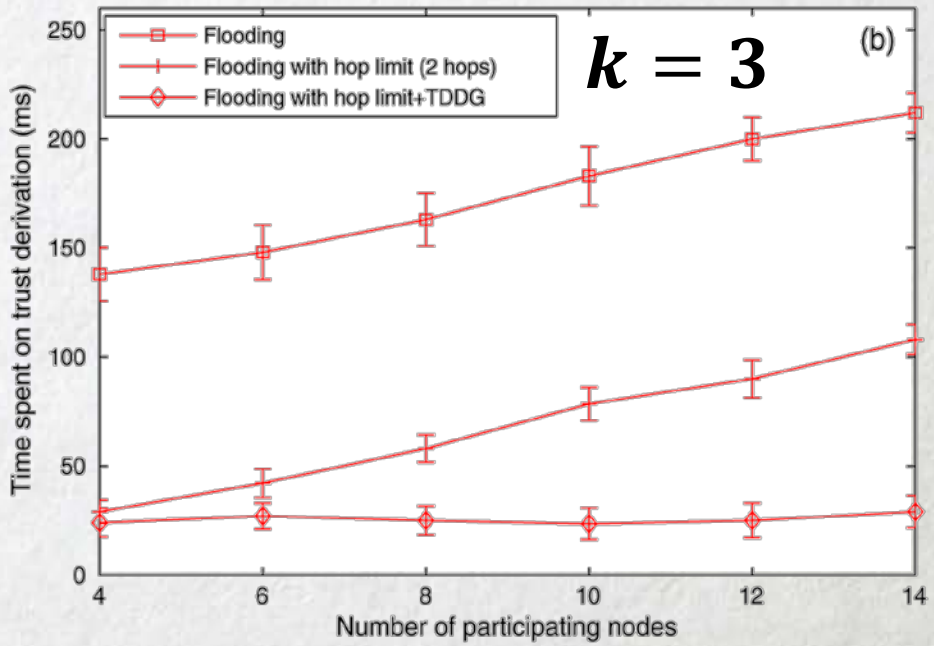




Simulation Results – Performance Evaluation

- the energy consumption produced by **flooding with hop limit** grows with the increasing number of participating nodes while the energy consumption of **TDDG approach** remains stable throughout.





Conclusions

- A **risk strategy model** is first proposed to determine the **optimal number of recommendations k that can satisfy the security requirements of a network**.
- Introducing the **Trust Derivation Dilemma Game**, **TDDG**, into the trust derivation process, **the probability of the selected strategy** was calculated based on the **mixed strategy Nash equilibrium** of the game.

Conclusions – Cont'd

- Compared with the traditional trust derivation methods, the simulation results showed that **the proposed game-theoretic approach can improve the performance of the network under the premise of security assurance, especially in a dense networks**.
- **Future work**: design trust derivation schemes by reducing the **overhead produced by trust request**, which can further improve the performance of the network.

Thank you for your kindly attention!

Q&A time