Tsinghua Science and Technology

Volume 18 | Issue 1 Article 12

2013

RISE: A Rellable and SEcure Scheme for Wireless Machine to Machine Communications

Wei Ren
Department of Information Security, School of Computer Science, China University of Geosciences, Wuhan 430074, China

Linchen Yu
Department of Information Security, School of Computer Science, China University of Geosciences, Wuhan 430074, China

Liangli Ma
Department of Computer Science, Naval University of Engineering, Wuhan 430030, China

Yi Ren
Department of Computer Science, "National" Chiao Tung University, Taiwan, China

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 12/12 pp100-117
Volume 18, Number 1, February 2013

RISE: A RelIable and SEcure Scheme for Wireless Machine to Machine Communications

Wei Ren*, Linchen Yu, Liangli Ma, and Yi Ren

Abstract: Wireless Machine to Machine (M2M) communications enable ubiquitous sensing, controlling, and acting via sensors, actuators, and actors. Reliability and security are of foremost importance in wireless M2M systems. A simple, target distinguishing attack can result in M2M's failure. This paper presents a RelIable and SEcure scheme, RISE, which is a package of policies that guarantee the reliability of data (including sensor reports and actuator instructions) and devices (including sensors, actuators, and actors). The data reliability is improved by four algorithms, ChooseMedian, ChooseMost, ChooseNearest, and Trust-based Enhancement. Report attainability is improved via m repeat-sending and n multiple-reporting algorithms. Device reliability is guaranteed by device-indistinguishability, which comprises data-indistinguishability and behavior-indistinguishability. The security requirements are formally defined, and the security analysis proves the soundness and completeness of the scheme.

Key words: Machine to Machine (M2M); reliability; security; target distinguishing attack

1 Introduction

Machine to Machine (M2M) communications may be the communication paradigm for many future applications such as the Internet of Things, wireless reactive sensor networks, and wireless network robotics[1-6]. The key difference between M2M and traditional communications is that M2M usually has no human involvement. Thus, it enables complete automation and adaptive control from far way to save labor and improve efficiency.

Since there is no human participation, M2M communications have critical problems in reliability and security that hinder large scale deployment. For example, when actors wait for instructions from actuators but all instructions are dropped in the communication channels, the actors will suspend for next operations. Or, if sensing results are all lost in the transmissions, the actuators will respon to the wrong control instruction and launch incorrect feedback. The reliability is, thus, of foremost importance due to the absence of double checking manually. Moreover, all sensing reports and instructions should maintain integrity to defend against modifications in the transmissions. Security is, thus, a basic requirement.

The reliability problem is also a challenge in the M2M context without human assistance, due to long distance transmissions, intermediate routing, and wireless tampering and sniffing. Moreover, if attackers can identify sensors, actuators, and actors, they can easily drop actuator instructions to terminate M2M controls.

M2M reliability and security is a new problem with some works starting to address user[7-11]. To the best of our knowledge, this paper makes the first attempt

• Wei Ren and Linchen Yu are with the Department of Information Security, School of Computer Science, China University of Geosciences, Wuhan 430074, China. E-mail: weirencs@cug.edu.cn; lichenyu@yahoo.com.cn.
• Liangli Ma is with the Department of Computer Science, Naval University of Engineering, Wuhan 430030, China. E-mail: maliangl@163.com.
• Yi Ren is with Department of Computer Science, "National" Chiao Tung University, Taiwan, China. E-mail: yiren@nctu.edu.tw.
∗ To whom correspondence should be addressed.
Manuscript received: 2012-11-10; accepted: 2012-12-12

to solve the reliability and security problem in M2M, especially using an approach with formal definitions and rigorous analysis.

2 Problem Formulation

2.1 Network model

There are three major entities in wireless M2M scenario, as depicted in Fig. 1.

(1) Sensors — wireless devices that sense or collect the required monitoring data, and report the data to actuator devices.

(2) Actuators — wireless devices that generate control or action instructions according to the received monitoring data, and report to actor devices.

(3) Actors — wireless devices that execute instructions sent from actuator devices.

The following concepts are defined:

Definition 1 Reports Sensing or monitoring data.

Definition 2 Instructions Control or action data.

Definition 3 Data Reports or instructions.

Definition 4 Devices Communication peers in the M2M system.

Definition 5 Sensors The peers send reports to actuators.

Definition 6 Actuators The peers receive reports from sensors, and send instructions to actors.

Definition 7 Actors The peers receive instructions from actuators.

These three devices are usually physically different. It is a typical scenario, in which the discussion can also be extended to other situations. Thus, in some cases, some entities may be one device physically, e.g., sensing and actor devices may be the same physical objects.

All devices access the network via wireless communications. The core network could be wired or wireless network.

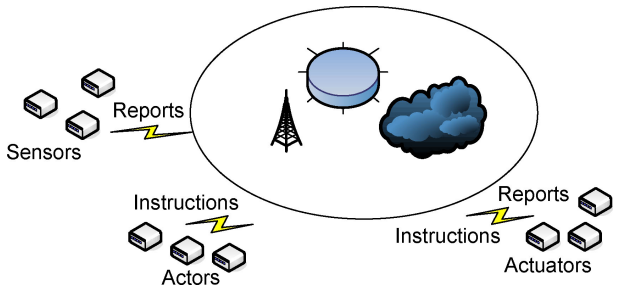


Fig. 1 Network model for wireless M2M.

2.2 Attack model, security requirements, and design goals

Adversaries reside in the communication channels between devices. They may sniff, modify, and forge data. Thus, the system must protect the confidentiality, integrity, and authenticity of the data.

The attackers in the channels may also recover a key used for data encryption and integrity. The system must provide resilience to key exposures. That is, the exposure of a key will not result in exposure of previous or future data.

In wireless M2M systems, the devices are exposed and can be captured or compromised by attackers. It is assumed that strong attacker exists who can physically hijack sensors to report wrong reports, or hijack actuators to send erroneous instructions.

Since the devices may also have energy constraints, the system will not rely the public key cryptosystems and a Trusted Third Party (TTP). The system is assumed to have pre-loaded pair-wise secret master keys on each device upon deployment.

The unique feature of M2M systems requires some further requirements for reliability and security in the following.

2.2.1 Data reliability

(1) Detection and deletion of authenticated but fake reports. Unauthenticated reports are fake. Some sensors may be compromised, thus authenticated reports may also be fake. The system must be able to discover and delete fake reports before actuators actually respond.

(2) Report attainability. If channels delete some reports, the reports can still reach actuators or the actuators can still respond properly.

(3) Detection and deletion of authenticated but fake instructions. Since the actuators may be compromised, instructions can be fake even though the instruction is authenticated. Thus, the system must be able to discover and delete fake instructions before actors execute those instructions.

(4) Instruction attainability. If channels delete some instrutions, the instrutions can still reach actors or the actors can still respond properly.

2.2.2 Device reliability

Definition 8 Target Distinguishing Attack The target distinguishing attack is a typical M2M attack that must be defended against because it can be easily launched by attackers. That is, if attackers can distinguish which devices are sensors, actuators, and actors, they will be able to easily launch such attack

by tampering the target's wireless signals, e.g., the actuator's channels, or simply dropping packets in the channels, e.g., reports or instructions, to result in abnormal M2M performance. If attackers can not distinguish between devices, they will have to tamper all device signals or drop all packets to cause M2M failure, which significantly increase the attack cost and detection possibility.

Indistinguishability of devices. The system must make it difficult for attackers to distinguish between the sensors, actuators, and actors. Indistinguishability requires two properties:

Indistinguishability of data. Attackers can not distinguish devices by observing the traffic patterns along the channels, such as the data length and data interval. Therefore, report lengths should be the same as instruction lengths.

Indistinguishability of behavior. Attackers can not distinguish devices by observing the communication patterns at the ends, such as data sending and receiving. Thus, the system should hide the events that sensors always send data, actors always receive data, and actuators both send and receive data.

2.2.3 Key exposure resilience

If the attackers in the channels gain access to the encryption and integrity keys, the data before and after the exposure should still remain secret and attain integrity.

The design goals are thus to develop a reliable and secure scheme for wireless M2M communications.

3 RISE Schemes

This section describe the components used to address the problems and achieve the design goals. Some of the major notation used in the remainder of the paper is listed in Table 1.

Table 1 Notation.

Symbol	Meaning
ID	Sensor identity
$\{\}_K$	Encryption by K.
K_{sa}	Sensor-actuator pairwise secret key
K_{aa}	Actuator-actor pairwise secret key
K_{i}	Transient integrity key
K_{c}	Transient cipher key
Report	Sensor result
Instruction	Actuator control statement to an actor
Data	Reports or instructions
Time	Time-stamp

3.1 Confidentiality and integrity protection

A simple scheme was developed to protect data confidentiality and integrity. Suppose each sensor-actuator pair shares a secret key K_{sa}. Besides, each actuator-actor pair shares a secret key K_{aa}. The report message format is thus:

$$\text{Sensor} \rightarrow \text{Actuator: } \{\text{ID, Report, Time}\}_{K_{\text{c}}},$$
$$\text{Hash(ID, Report, Time, } K_{\text{i}}).$$

Since the key used in the communication channel may be revealed by the attackers, the system always uses two transient keys K_{c} and K_{i}. They are generated by

$$K_{\text{c}} = \text{Hash}(K_{\text{sa}}, \text{Time}, 0), K_{\text{i}} = \text{Hash}(K_{\text{sa}}, \text{Time}, 1),$$

Similarly, the instruction is protected as follows:

$$\text{Actuator} \rightarrow \text{Actor: } \{\text{ID, Instruction, Time}\}_{K_{\text{c}}},$$
$$\text{Hash(ID, Instruction, Time, } K_{\text{i}}).$$

If reports or instructions are both denoted as Data, the protection can be rewritten uniformly as:

$$\text{Sender} \rightarrow \text{Receiver: } \{\text{ID, Data, Time}\}_{K_{\text{c}}},$$
$$\text{Hash(ID, Data, Time, } K_{\text{i}}).$$

3.2 Data reliability

3.2.1 Detection and deletion of authenticated but fake reports

Definition 9 Authenticated but Fake Report It is the report whose authenticity is verified by the message authentication code, but is indeed a fake report. Since sensors may be compromised by attackers, attackers can modify the report content before generation of the message authentication code. Thus, the report may be fake even though the report is authenticated.

Suppose the system deploys multiple sensors (instead of one) to report a monitoring event or an environmental parameter. Suppose n sensors report the event with values $v_1, v_2, \cdots, v_n$ to the actuator. If a value does not satisfy authentication verification, the value will be dropped. Otherwise, the actuator will detect and delete the fake report by the following policies.

Policy 1 Choose-Median Choose a median value as the final report. (1) Sort all n values from the largest to the least. (2) Output the value at position $n/2$. The algorithm is shown in Algorithm 1.

Algorithm 1 ChooseMedian Algorithm

Require: $v[1], v[2], \cdots, v[n]$
Ensure: *FinalReport*
$v[1], v[2], \cdots v[n] \Leftarrow Sort(v_1, v_2, \cdots, v_n)$
$FinalReport \Leftarrow v[\lfloor (n+1)/2 \rfloor]$

Sort() is a standard function, it is thus left as a subfunction to simplify the algorithm. The time complexity of the algorithm is the same as the sort function, $O(n^2)$.

Policy 2 Choose-Most Choose the value that is most reported. (1) Partition all n values into different sets, with each set having the same value. (2) Choose the set with the largest set size, and output the value in this set. The algorithm is shown in Algorithm 2.

Since partition function is not a standard function call, it is implemented in the algorithm. In this implementation, time complexity of algorithm is $O(n^2)$.

Policy 3 Choose-Nearest Choose the value that is nearest to the average. (1) Compute d_i for each value as $\bar{v} = \frac{\sum_{i=1}^{n} v_i}{n}$, $d_i = (v_i - \bar{v})^2$. (2) Sort d_i and choose the least one. The algorithm is shown in Algorithm 3.

The time complexity of Average() is $O(n)$. The time complexity of Sort() is $O(n)$. Thus, the time complexity of the algorithm is $O(n^2)$.

Policy 4 Trust-based Enhancement The detection accuracy is enhanced by utilizing the historical record from these three policies. The actuator maintains a trust table <ID, Trust> that records the heuristics, where ID is the sensor identity, and Trust indicates the possibility that sensor ID is a source of fake reports. Trust is measured by two metrics:

Metric 1 Number of verification failures This reflects the number of times that data has been modified along communication channels. A verification failure occurs when a received hash value does not equal the hash value calculated by the receiver. If data does not satisfy the verification check, Trust for that IDs is reduced by one.

Algorithm 2 ChooseMost Algorithm

Require: $v[1], v[2], \cdots, v[n]$
Ensure: *FinalReport*
  Partition $v[1], v[2], \cdots, v[n]$ into sets with the same value.
  for ($i = 1$ to n) **do**
    for ($j = i + 1$ to n) **do**
      if ($v[i]! = 0.AND.v[j] == v[i]$) **then**
        $v[j] \Leftarrow 0$
        $s[i] \Leftarrow s[i] + 1$
      end if
    end for
  end for
  Find the largest $s[i]$
  for ($i = 1$ to n) **do**
    if ($s < s[i]$) **then**
      $s \Leftarrow s[i]$
      $loc \Leftarrow i$
    end if
  end for
  $FinalReport \Leftarrow v[loc]$

Algorithm 3 ChooseNearest Algorithm

Require: $v[1], v[2], \cdots, v[n]$
Ensure: *FinalReport*
  $barv \Leftarrow Average(v[1], v[2], \cdots, v[n])$
  for ($i = 1$ to n) **do**
    $d[i] \Leftarrow (v[i] - barv)^2$
  end for
  Find the least $d[i]$
  for ($i = 1$ to n) **do**
    if ($d > d[i]$) **then**
      $d \Leftarrow d[i]$
      $loc \Leftarrow i$
    end if
  end for
  $FinalReport \Leftarrow v[loc]$

Metric 2 Number of deletions This reflects the probability of a device being compromised. The number of deletion is the number of times that the reported value from ID is not chosen by the Choose-Median, Choose-Most, or Choose-Nearest policies. In the Choose-Median Policy, the deletion values are the values not chosen. In the Choose-Most Policy, the deletion values are the values not in the chosen set. In the Choose-Nearest Policy, the deletion values are the values not equal to the chosen value. Trust for that ID will be reduced by one.

Trust-based Enhancement will then choose the ID with the highest Trust when multiple IDs exist after applying via Policies I, II, and III. The algorithm is shown in Algorithm 4.

The time complexity of the algorithm is still $O(n^2)$.

3.2.2 Report attainability

Definition 10 Report attainability This is the probability that the report on a given event from the sensors arrives at the corresponding actuator.

Report attainability can be improved by two policies:

Policy 5 *m* Repeat-Sending This improves the attainability by defending against the tampering attacks and packet dropping attacks in the communication channels. Each sensor sends each report m times. Even if some of them are dropped, the report still can reach to the actuator.

Policy 6 *n* Multiple-Reporting This improves the attainability by defending against sensor being

compromised together with packet dropping in the communication channels. This has already been proposed for detection and deletion of authenticated but fake reports. Since each event is reported by n sensors, the report attainability is improved even if some reports are dropped.

Proposition 1 If a channel randomly drops packets passing through the channel with probability p_{d}, the report attainability is $(1-p_{\mathrm{d}}^{mn})$ after m repeat-sending and n multiple-reporting.

Proof Packet dropping in channels occurs with a random probability p_{d}. There are $m \times n$ packets for the same event. Analyzing this as a Bernoulli experiment, the probability that all packets are dropped is p_{d}^{mn}. The probability that at least one packet is not dropped is, thus, $1-p_{\mathrm{d}}^{mn}$. ■

Besides, Repeat-Response policy will be used in case report attainability is zero. If the actors can not receive instructions, they will stop acting. To avoid this, the actuator will always send instructions, even when they have not received valid reports. If all the reports are faked or dropped by the communication channels, the actuators will repeat the last instruction. The instruction also encloses a tag that notifies the actor that this is a repeat instruction due to having no valid reports.

Finally, this method can also be applied to detection and deletion of authenticated but fake instructions for instruction attainability.

3.3 Reliability of devices

The security requirements are formally stated at first.

Algorithm 4 Trust-based Enhancement Algorithm

Require: $v[1], v[2], \cdots, v[n]$
Ensure: *FinalReport*
  FinalReport[1] $\Leftarrow$ *ChooseMedian*()
  FinalReport[2] $\Leftarrow$ *ChooseMost*()
  FinalReport[3] $\Leftarrow$ *ChooseNearest*()
  Actuator returns corresponding ID for a given value by checking the packet fields
  for $i = 1$ to 3 **do**
    $ID[i] \Leftarrow$ *ReturnID*(*FinalReport*[i])
  end for
  Find the largest $ID[i]$ in trust table
  for ($i = 1$ to 3) **do**
    if (*trust* < *Trust*[i]) **then**
      trust $\Leftarrow$ *Trust*[i]
      loc $\Leftarrow i$
    end if
  end for
  FinalReport $\Leftarrow$ *FinalReport*[*loc*]

Definition 11 Negligible function A function $u : \mathbb{N} \to (0,1)$ is said to be negligible if for every $c > 0$, for all sufficiently large n (for example, when $n > N$), $u(n) < 1/n^c$. We call $u(n)$ a negligible function and denote it as $\mathsf{negl}(n)$.

To simplify the following, the abstract notation called *-Indistinguishability or IND-* secure.

Definition 12 *-Indistinguishability(IND-* secure) If any Polynomial Time Turning Machine (PTTM) at the communication links can distinguish whether the sender is a sensor, actuator, or actor from Data with only a probability $\mathsf{negl}(n)$ (n is a security parameter), the scheme has the *-Indistinguishability property, or is IND-* secure. That is,

$$I(\text{CONJECTURE}; \text{OBSERVATION}) = H(\text{CONJECTURE}) - H(\text{CONJECTURE}|\text{OBSERVATION}) < \mathsf{negl}(n),$$

where $I(\cdot;\cdot)$ is mutual information; CONJECTURE is an event when attackers correctly conjecture the packet source (to be a sensor, actuator, or actor), OBSERVATION is the information collected by the attackers (that is data in the channels and behavior at the ends), $H(\cdot)$ is the entropy function, and "*" is a wild card character to represent any property.

As said in the security requirement section, the basic security requirement is Device-Indistinguishability (IND-DEVICE secure for short) to defend the target distinguishing attack. This requirement is satisfied using Data-Indistinguishability for data in the channel, and Behavior-Indistinguishability for the behavior at the ends. This leads to the following propositions.

Proposition 2 Device-Indistinguishability $\Leftrightarrow$ Data-Indistinguishability + Behavior-Indistinguishability,
where "$\Leftrightarrow$" means "equivalent".

Proof Straightforward. ■

Proposition 3 IND-DEVICE secure $\Rightarrow$ IND-DATA secure,
where "$\Rightarrow$" means "imply".

Proof Straightforward. ■

Proposition 4 IND-DEVICE secure $\Rightarrow$ IND-BEHAVIOR secure.

Proof Straightforward. ■

3.3.1 Data-Indistinguishability (IND-DATA)

To defend against the target distinguishing attack, attackers should not be able to distinguish devices by observing the data (traffic content and patterns) in the channels. The data information includes the length,

interval, and data linkages. The following policies are, thus, proposed:

Policy 7 Length-Indistinguishability (IND-LENGTH secure) For IND-LENGTH secure, the lengths of reports and instruction packets should be the same. This is already achieved by data confidentiality where the data is encrypted and the resulting ciphertexts have the same lengths.

Proposition 5 IND-DATA secure ⇒ IND-LENGTH secure.

Proof Straightforward. ■

Policy 8 Format-Indistinguishability (IND-FORMAT secure) Since the data packet format needs to be parsed by routers in the channels and can not be protected by data confidentiality, the packet formats for reports and instructions should be indistinguishable. This is also already achieved by data confidentiality, because the packet representation layer is ciphertext and the underlying layers are the same for both.

Proposition 6 IND-DATA secure ⇒ IND-FORMAT secure.

Proof Straightforward. ■

If M2M is enabled using IPv6 (e.g., 6LowPAN) and remotely accessible without network address translation, data packets can be routed in the communication channel. Attackers in the channels can thus observe some open fields in the packets such as the source address and destination address. Roughly speaking, the system should always hide patterns such as sensors always send data, actors always receive data, and actuators both send and receive data. The source addresses and destination addresses should also be equally presented.

Policy 9 Address-Indistinguishability (IND-ADDRESS secure) The number of different source addresses is equal to the number of different destination addresses. Thus, n sensors should send reports to n actuators and each report should be repeated m times. The n actuators have different addresses but share the same ID. Similarly, the n actuators also send instructions to n actors, with each instruction repeated m times. The n actors will also send n dummy packets to n sensors, with each repeated m times. Therefore, all the addresses used as source addresses and destination addresses will have the same occurrences. This policy is called Triangle Policy.

Proposition 7 IND-DATA secure ⇒ IND-ADDRESS secure.

Proof Straightforward. ■

Policy 10 Interval-Indistinguishability (IND-INTERVAL secure) The sending interval of all sensors for the same event are the same, denoted as I. The sending intervals for actuators and actors are also I. I is usually equal to or larger than the round trip time for the sensor-actuator-actor triangle. Any device can suspend for a random $r \in [0, S]$ seconds and then send out packets. If $S = 0$, I will be equal to the round trip time of the triangle (denoted as RTT). If $S > 0$, I will be larger than RTT. More specifically, I = RTT + $3S/2$ on average. This policy is called Same-Gap Policy.

Proposition 8 IND-DATA secure ⇒ IND-INTERVAL secure.

Proof Straightforward. ■

A nontrivial proposition will be proofed next to guarantee the completeness of the proposed policies.

Proposition 9 IND-LENGTH secure + IND-FORMAT secure + IND-ADDRESS secure + IND-INTERVAL ⇔ IND-DATA secure.

Proof Suppose a data packet has the form $\langle \text{plainfields}, \text{cipherfields} \rangle$. Since it is IND-LENGTH secure and IND-FORMAT secure, the packet can be simplified as $\langle \text{addr}_s, \text{addr}_d \rangle$, where in the plainfields the addr_s and addr_d are the representative fields. Since it is IND-ADDRESS secure and Triangle Policy is used, all addresses occur equally in addr_s and addr_d. Attackers, thus, can not distinguish sensors, actuators, and actors from the number of occurrences of addr_s and addr_d. Even if some data packets are dropped, distinguishing different devices is also hard due to the Triangle Policy. The Triangle Policy guarantees IND-DATA security in terms of space dimension, while the Same-Gap Policy guarantees IND-DATA security in terms of time dimension. Stated informally, the Triangle Policy makes the vertices indistinguishable, while the Same-Gap Policy makes different triangles indistinguishable. ■

3.3.2 Behavior indistinguishability

Attackers can not distinguish devices by observing the communication behavior at the ends. The attackers can sniff the communication behavior such as the lasting time and the intervals between sending signals. Thus, the system should hide the following patterns-sensors always send, actors always receive, and actuators both send and receive.

Policy 11 Send-Lasting-Indistinguishability (IND-SEND-LASTING secure) The lasting time (duration) for the sending behavior at each device

is the same. This is already implied by Length-Indistinguishability.

Proposition 10 IND-LENGTH secure ⇒ IND-SEND-LASTING secure.

Proof Straightforward. ■

Policy 12 Send-Interval-Indistinguishability (IND-SEND-INTERVAL secure) The number of sending behavior at each device is the same. This is already implied by Interval Indistinguishability.

Proposition 11 IND-INTERVAL secure ⇒ IND-SEND-INTERVAL secure.

Proof Straightforward. ■

Therefore, these two propositions lead to:

Proposition 12 IND-DATA secure ⇒ IND-BEHAVIOR secure.

Proof Straightforward. ■

3.4 Implementation details

The Triangle Policy and the Same-Gap Policy can be implemented by the following procedure.

(1) Deploy n sensors for monitoring each event. Also deploy p ($1 \leqslant p \leqslant n$) actuators that are related to these n sensors. These p actuators have n addresses. Then deploy q ($1 \leqslant q \leqslant n$) actors that also have n addresses and are related to the n sensors. This can be easily done in wireless channels. Therefore, regardless of the physical number of devices, a sensor-actuator-actor triangle can be assembled with $3n$ pairs of $\langle \text{addr}_\text{s}, \text{addr}_\text{d} \rangle$ with n addresses occurred in both addr_s and addr_d only once.

(2) Once an event happens, the n sensors will send reports to p actuators (or n virtual actuators). The p actuators will suspend for random $r_1 \in [0, S]$ seconds and then send the instructions to the q actors. The q actors will suspend for random $r_2 \in [0, S]$ seconds and then send dummy packets to the n sensors. The n sensors will suspend for random $r_3 \in [0, S]$ seconds before sending the next reports to the actuators.

(3) Even though some packets are dropped by the channels and do not reach the designated vertex, each vertex will always send n packets to the next vertex.

(4) Together with the m Repeat-Sending Policy, each vertex repeats the transmission of the same packet m times.

4 Related Work

The security of M2M communications is attracting much attention[9, 11], but there are few solutions. Lu et al.[11] first pointed out the reliability and security requirements in M2M communications. Fadlullah et al.[10] studied the detection of malicious activities in smart grid communications and proposed an early warning system. Bartoli et al.[8] studied secure aggregation in smart grid M2M networks. They included security designs in the physical layer and the MAC layer. Bartoli et al.[1] reviewed the current undergoing standards for M2M communications. Alam et al.[7] studied the interoperability in security attributes between different administrative domains in the Internet of Things with a layered architecture.

5 Conclusions

This paper described the critical security requirements for reliability of data and reliability of devices. An attack-target distinguishing attack in M2M is then defined. A confidentiality and integrity protection scheme is given for report and instruction. The data reliability is based on the four algorithms, ChooseMedian, ChooseMost, ChooseNearest, and Trust-based Enhancement. Report attainability is improved by implementing m repeat-sending and n multiple-reporting. Device reliability is guaranteed by device-indistinguishability, which includes data-indistinguishability and behavior-indistinguishability. A formal analysis of the security of the proposed schemes shows their soundness and completeness.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61170217), the Open Research Fund from the Shandong Provincial Key Laboratory of Computer Network (No. SDKLCN-2011-01), and Fundamental Research Funds for the Central Universities, China University of Geosciences (Wuhan) (No. 110109).

References

[1] A. Bartoli, M. Dohler, J. Serrano, A. Kountouris, and D. Barthel, Low-power low-rate goes long-range: The case for secure and cooperative machine-to-machine communications, *Lecture Notes in Computer Science*, vol. 61, no. 3, pp. 219-230, April 2011.

[2] K. Chang, A. Soong, M. Tseng, and Z. Xiang, Global wireless machine-to-machine standardization, *IEEE Internet Computing*, vol. 15, no. 2, pp. 64-69, March-April 2011.

[3] G. Lawton, Machine-to-machine technology gears up for growth, *Computer*, vol. 37, no. 9, pp. 12-15, September 2004.

[4] C. Wietfeld, H. Georg, S. Groening, C. Lewandowski, C. Mueller, and J. Schmutzler, Wireless communication

networks for smart grid applications, in *Proc. 11th European Wireless Conference 2011 - Sustainable Wireless Technologies (European Wireless)*, Vienna, Austria, April 2011, pp. 1-7.

[5] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. Johnson, M2m: From mobile to embedded internet, *IEEE Communications Magazine*, vol. 49, no. 4, pp. 36-43, April 2011.

[6] V. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, Home m2m networks: Architectures, standards, and qos improvement, *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44-52, April 2011.

[7] S. Alam, M. Chowdhury, and J. Noll, Interoperability of security-enabled internet of things, *Wireless Personal Communications*, vol. 61, no. 3, pp. 567-586, April 2011.

[8] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, Securelossless aggregation over fading and shadowing channels for smart grid M2M networks, *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 844-864, December 2011.

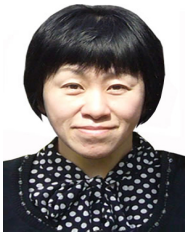
[9] I. Cha, Y. Shah, A. Schmidt, A. Leicher, and M. Meyerstein, Trust in M2M communication, *IEEE Vehicular Technology Magazine*, vol. 4, no. 3, pp. 69-75, September 2009.

[10] Z. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, An early warning system against malicious activities for smart grid communications, *IEEE Network*, vol. 25, no. 5, pp. 50-55, September-October 2011.

[11] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, Grs: The green, reliability, and security of emerging machine to machine communications, *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28-35, April 2011.

Wei Ren is currently an associate professor in School of Computer Science, China University of Geosciences (Wuhan), China. He was with Department of Electrical and Computer Engineering, Illinois Institute of Technology (IIT), USA in 2007 and 2008. He was a postdoctoral researcher fellowship in School of Computer Science, University of Nevada Las Vegas (UNLV), USA in 2006 and 2007. He was a research assistant in the Department of Computer Science, Hong Kong University of Science and Technology (HKUST) in 2004 and 2005. He received PhD degree in Computer Science from School of Computer Science and Technology, Huazhong University of Science and Technology (HUST), China. He received MEng and BEng degrees from University of Science and Technology Beijing in 1999 and 1996. He published more than 40 international journal papers. He is on the editorial broad of 4 international journals. His research interests include cryptography and network security.

Linchen Yu received her PhD from School of Computer Science and Engineering of Huazhong University of Science and Technology (HUST), China. She is now a lecturer in School of Computer Science of China University of Geosciences (Wuhan). Her research interests are peer-to-peer system and cloud computing.



Liangli Ma is a full professor and PhD supervisor in Department of Computer Engineering, Naval University of Engineering. She received PhD in Computer Science in School of Computer Science and Engineering, Huazhong University of Science and Technology. She has published 47 papers and 3 books, and obtained several awards for advancements in PLA. Her research interests include software assurance and security.

Yi Ren is currently doing research as a postdoctoral researcher at "National" Chiao Tung University (NCTU), Taiwan, China since 2012. He received his PhD in Information Communication and Technology from the University of Agder (UiA), Norway in 2012. His current research interests include security in wireless sensor networks, ad hoc, and mesh networks, LTE, smart grid, and e-health security. He received the Best Paper Award in IEEE MDM 2012.