Trust Management in Social Internet of Things: A Survey

Wafa Abdelghani[1(✉)], Corinne Amel Zayani[1], Ikram Amous[1], and Florence Sèdes[2]

[1] MIRACL Laboratory, Sfax University, Sfax, Tunisia
abdelghani_wafa@hotmail.fr,
{corinne.zayani,ikram.amous}@isecs.rnu.tn
[2] IRIT, Paul Sabatier University, Toulouse, France
florence.sedes@irit.fr

Abstract. Social Internet of Things is a new paradigm where Internet of Things merges with Social Networks, allowing people and devices to interact, facilitating information sharing and enabling a variety of at-tractive applications. However, face to this new paradigm, users remain suspicious and careful. They fear disclosure of their data and violation of their privacy. Without trustworthy technologies to ensure user's safe communications and trustworthy interactions, the SIoT will not reach enough popularity to be considered as a well-established technology. Accordingly, trust management becomes a major challenge to ensure reliable data analysis, qualified services and enhanced security. It helps people exceed their fears and promotes their acceptance and consumption on IoT services. However, current research still lacks a comprehensive study on trust management in SIoT. In this paper, we expose basic concepts, properties and models proposed for the trust management in SIOT environments. Furthermore, we discuss unsolved issues and future research trends.

Keywords: Social Internet of Things · Social networks · Trust management · Trust attacks

1 Introduction

The Internet of Things is expected to be dominated by huge content-oriented traffic, intensive interactions between billions of persons often on the move and heterogeneous communications among hosts and smart objects. It provision a millions of services, with strict real-time requirements and striking flexibility in connecting everyone and everything [13]. Interconnected things such as sensors or mobile devices sense, monitor and collect all kinds of data about human social life. Those data can be further aggregated, fused, processed, analyzed and mined in order to extract useful information to enable intelligent and ubiquitous services.

Integrating social networking concepts into the Internet of Things has led to the Social Internet of Things (SIoT) paradigm which enables people and connected devices to interact, facilitating information sharing and enabling a variety of attractive applications.

Y.K. Dwivedi et al. (Eds.): I3E 2016, LNCS 9844, pp. 430–441, 2016.
DOI: 10.1007/978-3-319-45234-0_39

However, face to this new paradigm, users remain suspicious and careful. They fear disclosure of their data and violation of their privacy. Without trust-worthy technologies to ensure user's safe communications, and trustworthy inter-actions, the SIoT paradigm will not reach enough popularity to be considered as a well-established technology, and all its potential will be lost.

Accordingly, trust management becomes a major challenge in SIoT to ensure reliable data analysis, qualified services and enhanced user's security. It helps people face and exceed their fears and uncertainty and promotes user's acceptance and consumption on IoT services and applications.

In the literature, trust mechanisms have been widely studied in various fields. However, existing models cannot be entirely applied in SIoT environments be-cause they are not adapted to its specific constraints (mobility, constrained re-sources,..). Current research has not comprehensively investigated how to man-age trust in such environments. This paper is a survey about the trust management in SIoT environments, its basic concepts, its properties, its models and its unsolved issues.

The paper is organized as follows. In Sect. 2, we expose an overview about the SIoT paradigm, its definitions, its evolution and its network structure. In Sect. 3, we address the notion of trust in SIoT environments, its properties, trust related attacks and the main constraints of trust management in SIoT. In Sect. 4, we present a classification of SIoT trust models. In Sect. 5, we provide literature review of trust models in Social Internet of Things. We conclude the paper in Sect. 6.

2 Social Internet of Things Paradigm

The Social Internet of Things (SIoT) is a new paradigm where IoT merges with social networks, allowing people and connected devices as well as the devices themselves to interact within a social network framework to support a new social navigation [12].

The structure of the SIoT network can be shaped as required to facilitate the navigability, to perform the discovery of objects and services and to guarantee the scalability like in human social networks. A level of trustworthiness must be established for leveraging the degree of interaction among things and social networks models can be adapted to address SIoT [9].

2.1 From Smart Things to Social Things

IoT embodies a large number of smart objects that, through standard communication protocols and unique addressing schemes, provide information and services to final users. Making objects smart was only the first step of an evolutionary process that affected modern communication devices and has been triggered by the advent of IoT in the telecommunication scenarios. The second step consists of the evolution of objects with a certain degree of smartness to objects with an actual social consciousness. These objects can interact with the surrounding environment and feature a pseudo-social behavior with "neighbors" or within "circles" and "communities".

The third step consists of the birth of social objects that act in a social com-munity of objects and devices [2]. Those social objects are able to autonomously establish relationships with other objects, to join communities and to build their own social network which may be different from their owners ones. This has given a specific structure to SIoT networks that is different from the structure of common social networks and that brings up new types of relationships.

2.2 SIOT Network Structure

[1, 3] address basic aspects to fully achieve an effective social networks of intelligent objects. In analogy with "human" social networks, [3] propose various forms of socialization among objects. The parental object relationship is defined among similar objects, built at the same period by the same manufacturer. Moreover, objects can establish co-location object relationship and co-work object relationship, like humans do when they share personal (e.g., cohabitation) or public (e.g., work) experiences. A further type of relationship is defined for objects owned by the same user (mobile phones, game consoles, etc.) that is named ownership object relationship. The last relationship is established when objects come into contact, sporadically or continuously, for reasons purely related to relations among their owners (e.g., devices/sensors belonging to friends); it is named social object relationship.

These relationships are created and updated on the basis of objects features (such as: object type, computational power, mobility capabilities, brand) and activity (frequency in meeting the other objects, mainly). Notice that, the establishment and the management of such relationships should occur without human intervention. Human is responsible only to set the rules of objects social interactions and then enjoys services resulting from such interactions.

Another structure was proposed by [6], who propose an SIOT network based on three kinds of social relationships connecting objects owners: (i) friendship relationship, which represents intimacy, (ii) social contact relationship, which represents closeness and proximity and (iii) community of interest relationship, which refers to common knowledge or experiences.

We note that when designing a structure for SIoT network, authors are divided between those who base on peer to peer networks and only opt for inter-objects social relationships and others who base on social networks and only consider social relationships between objects owners. However SIoT is a combination of both and should consider both objects and humans stakeholders. Thus, different kinds of relationships may operate between them such as: human-human, object-object and human-object social relationships.

3 Trust in Social Internet of Things

The concept of trust has been studied in many disciplines ranging from psychology to computer science. It is hard to precisely define the term "trust" because of its multidimensional, multidisciplinary and multifaceted aspects. A trust relationship involves at

least two entities: a trustor and a trustee, reliant on each other for mutual bene t and the context in which reside the trust relationship, such as the purpose of trust, the environment of trust (e.g., time, location, activity, devices being used, their operational mode, etc.), and the risk of trust. It specifies any information that can be used to characterize the background or the situation of involved entities [8]. Trust management is an important feature in networking systems like SIoT. We present here some properties of trust in general which depends on authors vision and hypothesis. Then we present specific challenges and constraints of trust management in SIoT environment.

3.1 Trust Properties

In literature, trust was computed in several ways depending on considered properties.

- **Trust can be direct:** This property says that trust is based on direct interactions, experiences or observations between the trustor and the trustee.
- **Trust can be indirect:** The trustor and the trustee here don't have any past experiences or interactions. The trust here is build on the opinion and the recommendation of other nodes. We talk about transitive trust.
- **Trust can be local:** It depends on the couple trustor/trustee considered and differs from one couple to another, which means that a node i can trust a node j whether another node k can distrust the same node j.
- **Trust can be global:** The global trust also called reputation means that every node has a unique trust value in the network which can be known by all other nodes.
- **Trust should be asymmetric:** Which means that two people tied by a relationship may have different levels of trustworthiness each other. The fact that A trusts B does not imply that B should trust A [13].
- **Trust should be subjective:** Trust is inherently a personal opinion which is based on various factors or evidence, and that some of those may carry more weight than others [10].
- **Trust can be objective:** In some case, such as when trust is computed based on QoS properties of a device.
- **Trust can be context-dependent:** Where the trust of a node i in a node j varies from one context to another.
- **Trust can be a composite property:** Trust is really a composition of many different attributes: reliability, dependability, honesty, truthfulness, security, competence, and timeliness, which may have to be considered de-pending on the environment in which trust has been specified [10].
- **Trust can depends on history:** This property implies that past experience may influence the present level of trust [16].
- **Trust should be dynamic:** Trust is non-monotonically changing with time. It may be periodically refreshed or revoked, and must be able to adapt to the changing conditions of the environment in which the trust decision was made [10].

3.2 Trust Related Attacks

A malicious node aims to break the basic functionality (e.g. service composition) of the IoT. In addition, it can perform the following trust-related attacks [5]:

1. **Self-promoting attacks (SPA):** it can promote its importance (by pro-viding good recommendations for itself) so as to be selected as the service provider, but then stop providing services or provide malfunction services.
2. **Bad-mouthing attacks (BMA):** it can ruin the reputation of well behaved nodes (by providing bad recommendations against good nodes) so as to decrease the chance of good nodes being selected as service providers.
3. **Ballot stuffing attacks (BSA):** it can boost the reputation of bad nodes (by providing good recommendations for them) so as to increase the chance of bad nodes being selected as service providers.
4. **Whitewashing attacks (WA):** a malicious node can disappear and rejoin the application to wash away its bad reputation.
5. **Discriminatory attacks (DA):** a malicious node can discriminatory at-tack non-friends or nodes without strong social ties (without many common friends) because of human nature or propensity towards friends in social IoT systems.
6. **Opportunistic service attacks (OSA):** a malicious node can provide good service to opportunistically gain high reputation especially when it feels its reputation is dropping because of providing bad service. With good reputation, it can effectively collude with other bad node to perform bad-mouthing and ballot stuffing attacks.

3.3 SIoT Trust Management Requirements/Constraints

SIoT networks are different from social networks because a large number of requirements and constraints such as characterizes them:

- Huge amount of entities and devices involved.
- Limited storage space capacity of entities and devices.
- Limited computation resources of entities and devices.
- High dynamism due to the large number of nodes joining and leaving the networks at any moment.
- Energy consumption, which is one of the biggest challenge of entities and device needing battery.
- Criticality and sensitiveness of used services and applications since they act on the real world.
- Power efficiency, making trust management algorithms and mechanisms faster and less energy consuming to support small things constraints.

Thus, trust management protocols must accommodate and ensure some important criteria such as scalability, adaptability, survivability, power efficiency and resiliency of the SIoT network.

4 SIoT Trust Models Classification

[11] propose to classify trust computation techniques on four design dimensions: trust composition, trust propagation, trust aggregation and trust update.

4.1 Trust Composition (TC)

In SIoT environment we distinguish two kind of trust based on the type of relationship: (i) the trust between a user and its device also known as quality of service (QoS) Trust and (ii) the trust between a user and other users also known as Social Trust. Trust composition refers to what factors to consider in trust computation especially QoS trust and social trust.

QoS Trust: QoS trust refers to the belief that an IoT device is able to provide quality service in response to a service request. QoS trust in general refers to performance and is measured by competence, cooperativeness, reliability, task completion capability, etc.

Social Trust: Social trust derives from social relationship between owners of IoT devices and is measured by intimacy, honesty, privacy, centrality, and connectivity, etc. Social trust is especially prevalent in social IoT systems where IoT devices must be evaluated not only based on QoS trust, but also based on the trust degree on their owners.

4.2 Trust Propagation (TP)

Trust propagation refers to how to propagate trust observations between entities. In general, there are two trust propagation schemes: (i) distributed and (ii) centralized.

Distributed: In the distributed trust propagation scheme, IoT devices prop-agate trust observations to other IoT devices they encounter or interact without the use of a centralized entity. The management of such propagation is arduous but it offers more scalability.

Centralized: The centralized trust propagation scheme requires the presence of a centralized entity (i.e. physical cloud) and uses structures like Distributed Hash Table (DHT).

4.3 Trust Aggregation (TA)

Trust aggregation consists of aggregating trust observations to get a unique convergent value. In the literature, the main aggregation techniques investigated are static weighted sum (SWS), dynamic weighted sum (DWS), Bayesian Model (BM) and Fuzzy Logic (FL).

4.4 Trust Update (TU)

Trust update concerns when trust is updated. In general, there are two schemes - event-driven scheme and time-driven scheme.

Event-Driven: In the event-driven scheme, all trust data in a node are updated after a transaction or an event is made.

Time-Driven: In the time-driven scheme, trust observations are collected periodically and trust is updated by applying a trust aggregation technique.

5 State of Art

5.1 Overview

Authors of [4] are the first to consider social relationships in trust management for IoT. They propose a new protocol based on three trust factors: (i) Honesty, (ii) Cooperativeness and (iii) Community interest. (i) Honesty refers to the belief of a node i that another node j is honest based on direct observations. Using a set of anomaly detection rules, node i count suspicious or dishonest experiences he had observed during a period Δ_t such as discrepancy in recommendation, interval, retransmission, repetition,… A dishonest node is a malicious node which aims to disturb the functionality and the performance of the IoT network giving improper recommendations to himself or to other nodes. (ii) Cooperativeness reflects the willingness of a node j to help other nodes in some task such as pro-viding a service to a service requester. An uncooperative node is not a malicious node. It does not aim to harm the basic functionality of IoT, but, it acts only for its own interest. [4] assume that friends are likely to be cooperative toward each other and compute cooperativeness value as the ration of the number of common friends over the total number of friends. (iii) Community interest represents the degree of common interest or same capabilities between two nodes and is computed as the ratio of the number of their common community/group interests over the total number of community/group interests.

Authors consider both direct and indirect trust. Direct trust is an aggregation of honesty, cooperativeness and community-interests values which are assigned by a node i to a node j based on direct observation and interaction between the two nodes. If the two nodes had never interacted in the past, the node i will consider the indirect trust which is based on the observations and the past experiences of other nodes with the concerned node. The honesty assessment and the indirect trust are used to increase the protocol resilience against some trust related attacks.

In summary, [4] propose a trust protocol which is both direct and transitive (indirect). The considered trust value is composite (depending on three factors), subjective and asymmetric (the trust of a node i in a node j differs from the trust of a node j in a node i). This value is dynamic because it varies over time and depend on history (past interactions) but not on the context. Trust values are aggregated with the static weighted sum and propagated in a distributed way.

Despite the fact that [4] are the first to consider social relationships in trust management for IoT, the proposed measure for computing cooperativeness (the percentage of common friends) is very simple and does not really reflect the willingness of a node i to cooperate and collaborate with others. The kind of social relationship exploited for measuring trust between object is the social relation-ship between their owners. However, in SIoT, an object is able to build its own social network which is different and independent of the social network of its owners. Furthermore the resiliency of the proposed protocol face to the trust related attacks has not been proven by evaluations. Finally, the proposed solution does not consider the specific constraints of the IoT environments such as storage management and energy consumption.

In [5], the authors aim at improving the trust management protocol pro-posed in [4]. They reuse the same trust measure, which is an aggregation of honesty, cooperativeness and community-interest. But they take into consideration other aspects such as the scalability, the adaptivity and the survivability of the protocol. As in the old protocol, the update of trust values is always events-driven and the trust values are computed only for a limited set of nodes to minimize computation and to maintain scalability. However, a new storage management strategy is proposed which permits to use limited storage space and to enhance scalability.

[6] propose an adaptive and scalable trust management protocol for SOA-based IoT systems. Distributed collaborating filtering technique is used to select trust feedback from owners of IoT nodes sharing similar social interests and three social relationships are considered for measuring social similarity and filtering trust feedback based on social similarity: (i) friendship, (ii) social contact, and (iii) community of interest. An adaptive filtering technique is employed for combining direct trust and indirect trust into the overall trust to minimize convergence time and trust bias of trust evaluation.

The proposed approach avoids Self-promoting, Bad-mouthing, Bal-lot stuffing and Opportunistic service attacks. It also take into consideration some SIoT constrains such as scalability and limited storage and computing capacity of IoT devices by computing trust only for the limited set of nodes of interest. However, authors don't consider social relationship between objects but only social relationship between their owners. The trust value is the same for all the objects and device owned by the same person. But the different characteristics of those different devices must influence the trust value. Moreover, QoS trust is not considered which is an important factor in Object-connected environments. Finally, considering a limited set of node is not a radical solution which can really ensure scalability. It is only a temporal solution.

[13] focused on the trustworthiness management in the social IoT by proposing subjective and objective approaches. The subjective approach has a slower transitory response, which is particularly obvious when dealing with nodes with dynamic behaviors. However, it is practically immune to typical behaviors of social networks, where a malicious person modifies his actions based on the relationships. On the contrary, the objective approach suffers from this kind of behavior, since a nodes trustworthiness is global for the entire network and this includes both the

opinion from the nodes with which it behaved maliciously and the opinion from the nodes with which it behaved benevolent. Direct service quality trust assessment and feedback propagation is used to avoid Self-promoting attacks. Credibility is used to avoid Bad-mouthing and Ballot stuffing attacks and quality trust assessment is used to remedy to Opportunistic service attacks. Distributed hash table are used for enhancing resiliency and scalability.

In [7] an access service recommendation scheme for efficient service composition and malicious attacks resistance in SIoT environments is proposed. To address issues in trustworthiness evaluation of SIoT services/devices including vulnerability, dynamic behavior, and resource restriction, they present a recommendation metric which integrated the timeliness properties of transactions and the social relationships between devices into the evaluation of access service in dynamic environment. An energy aware mechanism is also considered for workload balancing and network stability. The proposed approach permits to avoid Self-promoting and Bad-mouthing, Ballot stuffing. However, authors don't propose specific solutions for SIoT constraints such as scalability and limited storage and computational capacities. The presented works are classified and summarized in the Table 1.

Table 1. Classification of existing works based on SIoT network structure

	Human to Human social relationship	Object to Object social relationship
[5]		X
[6]		X
[13]	X	
[4]		X
[7]		X
[14]	X	
[15]		X

[14] proposed a trust service platform that offers trust evaluation of two any entities to SIoT services. Authors modulate the human trust information process and social relationship to create a trust model by incorporating three factors namely Reputation, Recommendation, and Knowledge. Recommendation represent surrounding suggestions (e.g. from friends, relatives, and colleagues) and reputation represent the global opinions on the trustee (e.g. ranking/ratings levels in public media). Knowledge is the information provided by trustee to evaluate its trustworthiness. Authors use ontology for representing user's knowledge which can be not suitable for limited resource objects. They don't explain how their protocol can face trust related attacks and don't propose solution to ensure the scalability of the SIoT network.

In [15], propose a trust model based on guarantor and reputation for SIoT environments. Every object has a reputation rating associated with it, which is stored in the object itself and which can only be updated by a reputation server. Agents are built into the objects to update the reputation. Objects are associated with their owners. If the owner buys a new object and associates it with oneself then that objects baseline reputation will be the same as other SIoT objects owned by the same person. The nodes use

credits to get services. If a node provides the correct service then he is paid some credits as commission. If he acts maliciously then it has to give some credits to the other nodes as forfeit payment. The commission and forfeit rates act as guarantees for an objects behavior. This approach ensure scalability because information about objects are stroked in a distributed way. However, it consider only social relationship between human and attribute the same trust value for all objects owned by the same person. Limitation of storage and computing capacity of objects as well as energy consumption are not taken into account.

5.2 Discussion and Comparison

In the previous subsection, we review the majority of work in the area of trust management on SIoT environments. We also highlight their limits. In this section, we provide a classification of those related work based on specific criteria. In Table 1, We compare them based on the involved SIoT network structure. In Table 2, we classify them based on adopted trust properties. In Table 3, we compare their resiliency face to the different kinds of trust related attacks. In Table 4, we compare them based on their willingness to respond to the specific SIoT constraints. And finally, in Table 5, we classify them according to Trust-Model dimensions.

Table 2. Classification of existing works based trust properties

	Direct	Indirect	Local	Global	Subjective	Objective	Asymmetric	Composite	Dynamic	Contextual
[5]	X	X	X		X		X	X	X	
[6]	X	X	X	X	X		X	X	X	
[13]		X		X	X	X	X	X		X
[4]		X		X	X		X		X	
[7]		X	X	X			X			
[14]		X		X			X	X		
[15]	X	X		X	X		X	X		

Table 3. Classification of existing works based resiliency face to trust related attacks

	SPA	BMA	BSA	OSA	DA	WA
[5]	X	X	X			
[6]	X	X	X			
[13]	X	X	X			
[4]	X	X	X			
[7]	X	X	X			
[14]	X	X	X	X		X
[15]	X					

Table 4. Classification of existing works based on considered SIoT constraints

	Scalability	Adaptability	Power efficiency	Survivability	Resiliency
[5]	X	X			X
[6]	X	X			X
[13]	X	X			X
[4]	X				X
[7]					X
[14]					X
[15]				X	

Table 5. Classification of existing works based on trust model dimensions

	Trust composition		Trust propagation		Trust aggregation				Trust update	
	QoS T	Social T	D	C	BM	SWS	DWS	FL	E-d	T-d
[5]	X	X	X				X		X	
[6]	X	X	X				X		X	X
[13]	X	X	X			X			X	
[4]	X	X	X			X			X	
[7]	X	X	X				X		X	
[14]		X	X					X	X	
[15]		X						X	X	

This comparison allow us to state that there is many progress in the area of Trust Management in SIoT systems. However, the majority of related works simply apply the trust protocols used in traditional social networks. These protocols prove their efficiency face to trust related attacks. But, they don't take into account, the novel structure and the novel constraints related to SIoT. Scalability is partially ensured and power efficiency is practically ignored. The majority of related works consider either human to human social relationship or object to object social relationship. However both of them are implied in this environments. A trust management protocol which is specifically designed for SIoT systems is still required.

6 Conclusion

In this survey, we pointed out the importance of trust management in SIOT. We first expose an overview about the SIOT paradigm, its evolutions and its network structure. Second, we address the trust notion and its related concepts. We demonstrate its role in SIOT environments and present its main properties.

Third, we present the main trust related attacks cited in literature. Fourth, we expose a classification of SIOT trust models based on specific criteria. Then, we provide a literature review of trust models in Social Internet of Things. Finally, we discuss unsolved issues.

References

1. Atzori, L., Iera, A., Morabito, G.: Siot: giving a social structure to the internet of things. IEEE Commun. Lett. **15**(11), 1193–1195 (2011)
2. Atzori, L., Iera, A., Morabito, G.: From "smart objects" to "social objects": the next evolutionary step of the internet of things. IEEE Commun. Mag. **52**(1), 97–105 (2014)
3. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The social internet of things (siot) when social networks meet the internet of things: concept, architecture and net-work characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
4. Bao, F., Chen, I.R.: Dynamic trust management for internet of things applications. In: Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, pp. 1–6. ACM (2012)
5. Bao, F., Chen, I.R., Guo, J.: Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In: 2013 IEEE Eleventh International Symposium on Autonomous De-centralized Systems (ISADS), pp. 1–7. IEEE (2013)
6. Chen, R., Guo, J., Bao, F.: Trust management for soa-based iot and its application to service composition. IEEE Trans. Serv. Comput. **2**(1), 1 (2015)
7. Chen, Z., Ling, R., Huang, C.M., Zhu, X.: A scheme of access service recommendation for the social internet of things. Int. J. Commun. Syst. (2015)
8. Dey, A.K.: Understanding and using context. Pers. Ubiquit. Comput. **5**(1), 4–7 (2001)
9. Geetha, S.: Social internet of things. World Sci. News **41**, 76 (2016). Avinashilingam
10. Grandison, T., Sloman, M.: A survey of trust in internet applications. IEEE Commun. Surv. Tutorials **3**(4), 2–16 (2000)
11. Guo, J., Chen, R.: A classification of trust computation models for service-oriented internet of things systems. In: 2015 IEEE International Conference on Services Computing (SCC), pp. 324–331. IEEE (2015)
12. Kim, J.E.: Architecting social internet of things. Ph.D. thesis, University of Pittsburgh (2016)
13. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social internet of things. IEEE Trans. Knowl. Data Eng. **26**(5), 1253–1266 (2014)
14. Truong, N.B., Um, T.W., Lee, G.M.: A reputation and knowledge based trust service platform for trustworthy social internet of things. Innovations in Clouds, Internet and Networks (ICIN), Paris, France (2016)
15. Xiao, H., Sidhu, N., Christianson, B.: Guarantor and reputation based trust model for social internet of things. In: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 600–605. IEEE (2015)
16. Yan, Z., Holtmanns, S.: Trust modeling and management: from social trust to digital trust, pp. 290–323. IGI Global (2008)