Formal Context Aware Secure Framework for Sensor Network Environment

Pooja Mohan[#],
[#]Department of IT, GGDSD College, Panjab University, Chandigarh, India

Manpreet Singh[*],
[*]University College of Engineering, Punjabi University, Patiala, India

***Abstract* ---- A wireless sensor network is defined as a large collection of sensor nodes, each equipped with its own sensor, processor and radio transceiver having data acquisition and data processing capabilities. The most important features in Wireless Sensor Network makes it different from other network; self-organize, low power, low memory, low bandwidth for communication, large-scale nodes, self-configurable, wireless, infrastructure-less. Wireless sensor networks (WSNs) are an enabling technology of context-aware systems. To provide personalized services, we should consider both user's privacy and security requirements within context-awareness environment. Traditional authentication and access control mechanisms are independent of context i.e. they do not adapt themselves with changing context. Devices, services in dynamic environments automatically adapt to changing contexts. In this paper context aware model to provide security in sensor environment is proposed.**

Keywords --- Security, Access control, Context, Sensor Network

I. INTRODUCTION

The increasing development in wireless mobile communications has attracted an important amount of attention on the security, anonymity and privacy issues. Designing secure systems require one to understand what resources an entity has access to and how to provide privacy and confidentiality. In traditional models, authentication and access control were context-less and depend on static credentials of the user and objects. Moreover, as the availability of contextual information may introduce new threats against security and privacy, it can also be used to improve dynamic aspects of security, and privacy.

Authentication, Access Control, and Privacy refer to the problems of ensuring that communications takes places in a secure manner and only between the right parties without disclosure of information to unauthorized eavesdroppers. Authentication services are of two main types; one is e-authentication by which a user is identified through the use of an eToken, and the other is physical authentication (p-authentication) by which a user is identified through the use of biometrics, sensors, or location based services.

The purpose of access control is to limit the operations that a legitimate user of a computer system can perform. In this way, access control seeks to prevent activity that could lead to a breach of security. Correctly establishing the identity of the user is the responsibility of the authentication service. Access control refers to limiting what users can do after they identify themselves and are authenticated.

II. RELATED WORK

The definition of context includes any information that describes physical objects, applications and users in any domain. Context information varies in different applications areas. The term "context" is defined as "any information that can be used to characterize the situation of an entity" [1]. This definition is traditionally linked with the design of context-aware applications, where contexts are information that describes the situation of any entity relevant to the application.

The applications are context consumers that receive information from context producers, and produce their own context that they provide to other context consumers (e.g., other applications). By exchanging contexts, the applications can adjust their behaviors according to contexts to optimize their performance. Context may be of low level or high level. High level contexts can represent the status of a node, network, or system, while low level contexts can describe the status about the parts of a node, network, or system. [2]

Context modeling refers to the process of creating an abstract representation of situations in the real-world such that it can be interpreted and exchanged by machines. Context information can be represented by various methods as Graphical Models, Spatial context model, Logic Based Models; Ontology based models, Key Value Models and Markup Scheme Models. [3]

A number of context-aware designs for WSNs have been proposed based on context awareness such as network routing [4-5], storage allocation [6] and energy management [7]. Both the context toolkit [8] and the sensor architecture of Schmidt et al. [9] support the acquisition of context data from sensors, and the processing of this raw data to obtain high-level context information. The former is a programming toolkit that can be connected together to gather and process context information from sensors. The latter provides a layered model of context processing in which sensor output is transformed into one or more cues, which undergo processing to form an abstract context description comprising a set of values, each associated with a certainty measure that estimates the certainty that the value is correct.

A number of alternate models have been proposed to provide security in sensor environments. One such model is Role Based Access Control (*RBAC)*. RBAC is an alternative to traditional Discretionary (DAC) and mandatory access control (MAC). In RBAC users are assigned roles and roles are assigned permissions. Sandhu [10] et al defines RBAC model as RBAC0, RBAC1 and RBAC2, where RBAC0 is a model with user associated with roles and roles with permission. RBAC1 is RBAC0 with role hierarchies and RBAC2 is RBAC1 with constraint on user/role, role/role and role/permission. Other factors such as time, location, etc. are not considered in making access control decision in these models. Later on, several extended access control schemes have been proposed. M. Covington [11] proposed Generalized RBAC by defining three types of roles subject, environment and object roles and it uses context information in making access decision. Zhang [12] proposed dynamic RBAC model where users' role are activated dynamically based on context changes in each session. Two state machines are defined one for users' role and another for permission. As it is impossible to generate machines for various users and objects so this model is not appropriate.

Context model based on RBAC [13] defines four context management roles: Context owner, Context provider, context broker and context aware service provider. There focus is on collection management and interpretation of context information. Securities policies specification with contextual condition is not supported by this model.

Cerebus [14] proposed four components security service, context infrastructure, a knowledge base and inference engine with context policies based on first order logic. Since there are various rules so due to complexity of rule management and also delay in fetching context this model is not suitable for real time environment. Tianjie C. et al [15] present a flexible access control model with dynamically grants and adapt permissions to users based on context information including time, location and trust value.

Jafarian [16] proposed a context aware mandatory access control model which can be deployed in multilevel security environments, where context information is in form of predicates and context types. It is only suited for environments such as military ones.

III. CONTEXT AWARE SECURE FRAMEWORK

A. Context-Awareness

Contexts can be classified into two categories - direct context and indirect context based on the means by which context is obtained. Direct context is acquired from either physical sensors or is defined by the user. Indirect context is obtained by aggregation and reasoning process. Context can be deduced from context reasoning engine. For example a person is in meeting can be deduced by collecting contexts such as if he is at meeting location, and his current time is the scheduled interval for meeting.

System, Environment, Temporal and User contexts are four classes of contexts already defined by study [17]. According to study system context includes information relating to computing system which vary according to different layers of OSI model. The information Work flow status would be for application layer, IP address and Routing information for network layer. Environmental context consist of any kind of context information related to the physical environment. Environmental context information includes e. g., lighting, temperature, weather, noise, humidity etc. Temporal context defines any kind of context information related to time. Time of day, month and year are typical temporal context information. User context refers to any kind of context information related to the user such as user's age, location, medical history, Biometric information, such as fingerprint, iris or face shape.

Data for an application may be context information or main data element. Ex. Room temperature is main data for climate control system and context information if obtained through body sensors. In wireless computing environment Contextual information can come from different network locations, protocol layers and device etc.

B. Context awareness for wireless sensor network

WSN nodes must be able to adapt to their context (for example, their energy level). The context is a set of information that the node may have on its environment. A node takes into account its context to improve its lifetime and consequently the overall functioning of the network.

In a Wireless Sensor Network, concept of context can be used to improve the security of the network. The context can be anything; it may be some attribute of sensor node. In Wireless Sensor network, whenever some new node enters from outside environment, there may be some risks to security. So, how to secure such a network is the primary concern. Whenever a node enters, some negotiations are made with all other nodes already present in the network based on some common attributes of node. These negotiations establish a level of trust between various nodes. On the basis of which it can be identified which nodes are secure. These attributes may be anything depending upon the application in which sensor nodes are deployed. These are some of the attribute of sensor environments.

The **device context** provides knowledge about local device conditions, such as the energy state, storage level, CPU usage, battery level, time stamp, IP address, bandwidth, Device mode (sleep/wake), transmitting power and services provided by a node. **The network context** represents network wide situations and states, such as network topology, overall transmission capacity, or path qualities in the network. The **system context** represents status of the system, such as the current executing tasks of an application or the state of the system performance, which can be shared with the underlying network. The **environment context** provides knowledge for a network to understand the changes of its environmental properties or attributes, such as temperature, Pressure, Humidity, noise, Lighting, season, and occurrence of a fire incident. Various

types of context may also be included according to the system specifications. **Person Context** represents exact location, physical parameters measured from sensors, User role, location of source, direction, speed etc.

Communication Context includes description about the state of a node's communication which can be in terms of the general quality, efficiency, security, frequency, availability, or pattern of communication includes packet overhead, throughput, link capacity, and quality of service (QoS), signal strength. **Service Context** includes Domain, time period for communication, Exact Location, time stamp, Requesting party identity, service provider destination role, location of destination, Scenario, trustworthiness. **Location Context** includes Physical coordinates, Meaningful location for the user – home, office, hospital, gym etc.

C. *Model description*

There are various contextual elements in this model.
Let C be the set of contexts collected through sensors and inferred through various reasoning techniques.

C= { $C_1, C_2, C_3, \ldots . C_N$}

C_1 : DeviceContext= {Energy state, Storage level, CPU usage, IP address, Bandwidth}
C_2: NetworkContext = {Network topology, Transmission capacity}
C_3 : EnvrContext = {Temperature, Pressure, Humidity, Noise, Lighting, Season}
C_4 : CommCntext = {Quality, Efficiency, Security, Frequency, Availability, Packet overhead, Throughput, link capacity, quality of service (QoS), Signal strength}
C_5 : ServiceContext= {Domain, time period, Exact Location, time stamp}
C_6: LocContext = {Physical coordinates, location for the user}

By represented relation between these sets how they are interrelated with each other we can determine Context Conditional constraint as a Boolean expression to represent security requirements for a sensor network, which is the logical conjunction of explicit conditions.

ContextCC= $\cup_{i=1}^{j}(CC_j)$

$$CC = \bigcap_{i=1} j\ SubC_i$$

SubC: = $< C >< OP >< VAL >$
Where OP={$>, <, \leq, \geq, =, \neq$}
If C= {time, location}
Ex. Patient record can be accessed from hospital between 9:00 and 5:00
ContextCC= $(time \geq 9{:}00 \cap time < 18{:}00 \cap location\ in\ hospital$
Security rule can be defined as SR=(C, P, ContextCC)
Where C is context set, P is permission to be assigned and ContextCC is context conditional constraint. Authorization permission is a policy that decides whether user access request is allowed in a given session. Access request is a user request to access a particular resource.
We can define security evaluation function (SEF) which grants permission to context for which the context conditional constraint evaluates to true otherwise permission will be denied.
SEF→ $\{Grant, Deny\}$
Security information is a collection of various security parameters and security functions. This information is the collection of various security policies rules i.e. trust based, context based etc. Security functions are defined on the basis of these policies. The access is granted if security function evaluates to true otherwise it is denied.
Security Evaluation Function is defined as
SEF(ac): P→D
Where P= {p_1,p_2,…..,p_3} is set of policies
D= {Grant, Deny}

Algo: AccessRequest ( )
if (ContextCC( ) is true)
result = "Grant"
break
else
result = "Deny"
end if
return result

IV. CONCLUSION

In this paper we proposed model based on context information. In addition we presented the formal definitions for context, context conditional constraints etc. The context aware secure model for sensor environment is presented. In this various contextual parameters of wireless sensor network is defined. Future research activities will be devoted to implement and evaluate the proposed ontology-based context model and logic-based context reasoning schemes in WSN environments.

REFERENCES

1. Dey, A. K. (2001), "Understanding and using context", *Personal and ubiquitous computing*, *5*(1), 4-7.
2. Liu, Y., Seet, B. C., & Al-Anbuky, A. (2013), "An Ontology-Based Context Model for Wireless Sensor Network (WSN) Management in the Internet of Things". *Journal of Sensor and Actuator Networks*, *2*(4), 653-674.
3. Mohan, P., & Singh, M. (2013), "Formal Models for Context Aware Computing", *International Journal of Computer Applications Technology and Research*, *2*(1), 53-58.
4. Koo, B., Won, J., Park, S., & Eom, H. (2009), "PAAR: A routing protocol for context-aware services in wireless sensor-actuator networks", In *Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on* (pp. 1-7). IEEE.
5. Haque, M., Matsumoto, N., & Yoshida, N. (2010), "Utilizing multilayer hierarchical structure in context aware routing protocol for wireless sensor networks. *Int. J. Comput. Sci*, *4*, 23-37.
6. Kim, H., Park, J., Seong, D., & Yoo, J. (2011), "A Context Aware Data-Centric Storage Scheme in Wireless Sensor Networks". In *Multimedia, Computer Graphics and Broadcasting* (pp. 326-330). Springer Berlin Heidelberg.
7. Gladisch, A.; Daher, R.; Lehsten, P.; Tavangarian, D. (2011), "Context-Aware Energy Management for Energy-Self-Sufficient Network Nodes in Wireless Mesh Networks". In Proceedings of the

3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Budapest, Hungary, 5–7 October 2011.

8. Dey, A., Salber, D., Abowd, G. (1999), "A context-based infrastructure for smart environments", in: 1st International Workshop on Managing Interactions in Smart Environments (MANSE'99). pp. 1-15.
9. Schmidt, A., Aidoo, K. A., Takaluoma, A., Tuomela, U., Van Laerhoven, K., & Van de Velde, W. (1999), "Advanced interaction in context". In *Handheld and ubiquitous computing* (pp. 89-101). Springer Berlin Heidelberg.
10. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996), "Role-based access control models", *Computer*, *29*(2), 38-47.
11. Covington, M. J., Moyer, M. J., & Ahamad, M. (2000), "Generalized role-based access control for securing future applications"
12. Zhang, G., & Parashar, M. (2004), "Context-aware dynamic access control for pervasive applications", In *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference* (pp. 21-30).
13. Hulsebosch, R. J., Salden, A. H., Bargh, M. S., Ebben, P. W., & Reitsma, J. (2005), "Context sensitive access control", In *Proceedings of the tenth ACM symposium on Access control models and technologies* (pp. 111-119). ACM.
14. Al-Muhtadi, J., Ranganathan, A., Campbell, R., & Mickunas, M. D. (2003). Cerberus: a context-aware security scheme for smart spaces. In *Pervasive Computing and Communications, 2003.(PerCom 2003). Proceedings of the First IEEE International Conference on* (pp. 489-496). IEEE.
15. Li, L., & Cao, T. (2008), "A Flexible, Autonomous and Non-redundancy Access Control for Ubiquitous Computing Environment", In *Information Science and Engineering, 2008. ISISE'08. International Symposium on* (Vol. 1, pp. 446-450). IEEE.
16. Jafarian, J. H., Amini, M., & Jalili, R. (2009). CAMAC: A Context-Aware Mandatory Access Control Model. *ISeCure, The ISC International Journal of Information Security*, *1*, 35-54.
17. Wrona, K., & Gomez, L. (2005), "Context-aware security and secure context-awareness in ubiquitous computing environments", In *XXI Autumn Meeting of Polish Information Processing Society*. pp. 255-265