РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2007 106 614** (13) **A**

(51) МПК
H04L 12/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2007106614/09, 22.02.2007**

(43) Дата публикации заявки: **27.08.2008 Бюл. № 24**

Адрес для переписки:
117393, Москва, ул.Профсоюзная, 78, оф.3323, СТАРФИЛД, пат.пов. В.Н.Рослову

(71) Заявитель(и):
Корпорация "САМСУНГ ЭЛЕКТРОНИКС Ко., Лтд." (KR)

(72) Автор(ы):
Чмора Андрей Львович (RU),
Уривский Алексей Викторович (RU),
ЖЕОНГ Хьюн Йи (KR)

(54) СИСТЕМА РОБАСТНОГО УПРАВЛЕНИЯ КЛЮЧАМИ И СПОСОБ ЕЕ ФУНКЦИОНИРОВАНИЯ

(57) Формула изобретения

1. Система робастного управления ключами для обслуживания сети с кластерной архитектурой, использующая доверенный центр на этапе формирования и распределения ключевых блоков и распределенный центр управления ключами для поддержания режима полноценного функционирования, обеспечивающая высокий уровень секретности и отказоустойчивости за счет согласованного применения схем EKSYD и CuBES, имеющая гарантированную защищенность при межкластерном и внутрикластерном взаимодействии узлов без участия доверенного центра и распределенного центра управления ключами, в которой доверенный центр имеет исполнительную схему процессора, генератор псевдослучайных чисел, память и приемопередатчик; распределенный центр управления ключами имеет исполнительную схему процессора, генератор псевдослучайных чисел, память и приемопередатчик, а каждый узел сети имеет исполнительную схему процессора, память и приемопередатчик, при этом:

доверенный центр выполнен с возможностью исполнения всех необходимых подготовительных вычислений с последующим формированием посредством исполнительной схемы процессора ключевого пула и ключевых блоков схемы EKSYD;

доверенный центр выполнен с возможностью исполнения всех необходимых подготовительных вычислений с последующим формированием посредством исполнительной схемы процессора ключевого пула и ключевых блоков схемы CuBES;

доверенный центр выполнен с возможностью секретной передачи посредством каналов связи сформированных упомянутых совокупных ключевых блоков, состоящих из ключевых блоков схем EKSYD и CuBES, узлам каждого кластера, участвующих в межкластерном и внутрикластерном взаимодействии, а также управляющим узлам;

управляющие узлы выполнены с возможностью осуществления посредством исполнительной схемы процессора и приемопередатчика процедуры периодического обновления совокупных ключевых блоков узлов, включая управляющие узлы, при помощи схемы EKSYD;

управляющие узлы выполнены с возможностью осуществления посредством исполнительной схемы процессора и приемопередатчика процедуры отключения скомпрометированных узлов через обновление совокупных ключевых блоков нескомпрометированных узлов при условии, что число этих узлов не превышает порога

RU 2007106614 A

RU 2007106614 A

компрометации схемы EKSYD, при помощи схемы EKSYD;

управляющие узлы выполнены с возможностью осуществления посредством исполнительной схемы процессора и приемопередатчика процедуры отключения скомпрометированных узлов через обновление совокупных ключевых блоков нескомпрометированных узлов, за исключением управляющих узлов, при условии, что число этих узлов превышает порог компрометации схемы EKSYD, при помощи схемы CuBES;

управляющие узлы выполнены с возможностью осуществления посредством исполнительной схемы процессора и приемопередатчика процедуры отключения скомпрометированных управляющих узлов через обновление совокупных ключевых блоков нескомпрометированных управляющих узлов при условии, что число этих узлов не превышает порог компрометации схемы EKSYD, при помощи схемы EKSYD;

узлы mesh-сети выполнены с возможностью формирования посредством упомянутой исполнительной схемы процессора общего секретного ключа на основе ключей из совокупного ключевого блока узла-отправителя и информации о ключах из совокупного ключевого блока узла-получателя;

узлы mesh-сети выполнены с возможностью шифрования/дешифрования полезной информации на общем секретном ключе посредством упомянутой исполнительной схемы процессора;

узлы mesh-сети выполнены с возможностью передачи/приема сформированного сообщения посредством упомянутого приемопередатчика;

узлы mesh-сети выполнены с возможностью приема посредством упомянутого приемопередатчика широковещательных сообщений от управляющих узлов;

узлы mesh-сети выполнены с возможностью проверки подлинности принятых широковещательных сообщений от управляющих узлов и их последующего дешифрования посредством упомянутой исполнительной схемы процессора;

узлы mesh-сети выполнены с возможностью формирования обновленого ключевого блока на основе принятой от управляющих узлов информации посредством упомянутой исполнительной схемы процессора.

2. Система робастного управления ключами по п.1, отличающаяся тем, что доверенный центр выполнен с возможностью формирования ключевых пула и блоков схемы CuBES.

3. Система робастного управления ключами по п.1, отличающаяся тем, что доверенный центр выполнен с возможностью секретной передачи совокупных ключевых блоков узлам каждого кластера на этапе развертывания сети.

4. Система робастного управления ключами по п.1, отличающаяся тем, что распределенный центр управления выполнен с возможностью периодического обновления совокупных ключевых блоков узлов при помощи схемы EKSYD.

5. Система робастного управления ключами по п.1, отличающаяся тем, что распределенный центр управления выполнен с возможностью изолирования скомпрометированных узлов при помощи схемы EKSYD.

6. Система робастного управления ключами по п.1, отличающаяся тем, что распределенный центр управления выполнен с возможностью изолирования скомпрометированных узлов при помощи схемы CuBES.

7. Система робастного управления ключами по п.1, отличающаяся тем, что узлы выполнены с возможностью формирования парного секретного ключа на основе ключей из совокупного ключевого блока узла-отправителя и информации о ключах из совокупного ключевого блока узла-получателя.

8. Способ функционирования системы робастного управления ключами, состоящий из следующих операций:

формируют посредством исполнительной схемы процессора доверенного центра ключевой пул и ключевые блоки схемы EKSYD;

формируют посредством исполнительной схемы процессора доверенного центра ключевой пул и ключевые блоки схемы CuBES;

секретно передают посредством каналов связи доверенного центра совокупные ключевые блоки, состоящие из ключевых блоков схем EKSYD и CuBES, узлам каждого

RU 2007106614 A

RU 2007106614 A

кластера;

формируют посредством исполнительной схемы процессора доверенного центра совокупный ключевой блок управляющих узлов распределенного центра управления;

осуществляют посредством исполнительной схемы процессора и приемопередатчика управляющих узлов распределенного центра управления периодическое обновление совокупных ключевых блоков узлов, включая управляющие узлы, при помощи схемы EKSYD;

осуществляют посредством исполнительной схемы процессора и приемопередатчика управляющих узлов распределенного центра управления отключение скомпрометированных узлов через обновление совокупных ключевых блоков нескомпрометированных узлов при условии, что число этих узлов не превышает порога компрометации схемы EKSYD, при помощи схемы EKSYD;

осуществляют посредством исполнительной схемы процессора и приемопередатчика управляющих узлов распределенного центра управления отключение скомпрометированных узлов через обновление совокупных ключевых блоков нескомпрометированных узлов, за исключением управляющих, при условии, что число этих узлов превышает порог компрометации схемы EKSYD, при помощи схемы CuBES;

осуществляют посредством исполнительной схемы процессора и приемопередатчика управляющих узлов распределенного центра управления отключение скомпрометированных управляющих узлов через обновление совокупных ключевых блоков нескомпрометированных управляющих узлов при условии, что число этих узлов не превышает порога компрометации схемы EKSYD, при помощи схемы EKSYD;

формируют посредством упомянутой исполнительной схемы процессора узла общий секретный ключ на основе ключей из совокупного ключевого блока узла-отправителя и информации о ключах из совокупного ключевого блока узла-получателя;

шифруют/дешифруют полезную информацию на общем секретном ключе посредством упомянутой исполнительной схемы процессора узла;

передают/принимают сообщения посредством упомянутого приемопередатчика узла;

принимают посредством упомянутого приемопередатчика узла широковещательные сообщения от управляющих узлов распределенного центра управления;

проверяют подлинность принятых широковещательных сообщений от управляющих узлов распределенного центра управления и дешифруют эти сообщения посредством упомянутой исполнительной схемы процессора узла;

формируют обновленный совокупный ключевой блок на основе принятой от управляющих узлов распределенного центра управления информации посредством упомянутой исполнительной схемы процессора узла.

9. Способ по п.8, отличающийся тем, что формируют ключевой пул и блоки в соответствии с конструкцией схемы EKSYD.

10. Способ по п.8, отличающийся тем, что формируют ключевой пул и блоки в соответствии с конструкцией схемы CuBES.

11. Способ по п.8, отличающийся тем, что секретно передают совокупные ключевые блоки узлам каждого кластера.

12. Способ по п.8, отличающийся тем, что выполняют периодическое обновление совокупных ключевых блоков при помощи схемы EKSYD.

13. Способ по п.8, отличающийся тем, что выполняют отключение скомпрометированных узлов при помощи схемы EKSYD.

14. Способ по п.8, отличающийся тем, что выполняют отключение скомпрометированных узлов при помощи схемы CuBES.

15. Способ по п.8, отличающийся тем, что формируют парный секретный ключ на основе ключей из совокупного ключевого блока узла-отправителя и информации о ключах из совокупного ключевого блока узла-получателя.

RU 2007106614 A

RU 2007106614 A